Topology of Numbers

Allen Hatcher

Chapter 0: A Preview

Pythagorean Triples

As an introduction to the sorts of questions that we will be studying, let us consider right triangles whose sides all have integer lengths. The most familiar example is the $(3,4,5)$ right triangle, but there are many others as well, such as the $(5,12,13)$ right triangle. Thus we are looking for triples (a,b,c) of positive integers such that $a^2+b^2=c^2$. Such triples are called *Pythagorean triples* because of the connection with the Pythagorean Theorem. Our goal will be a formula that gives them all. The ancient Greeks knew such a formula, and even before the Greeks the ancient Babylonians must have known a lot about Pythagorean triples because one of their clay tablets from nearly 4000 years ago has been found which gives a list of 15 different Pythagorean triples, the largest of which is $(12709,13500,18541)$. (Actually the tablet only gives the numbers a and c from each triple (a,b,c) for some unknown reason, but it is easy to compute b from a and c.)

There is an easy way to create infinitely many Pythagorean triples from a given one just by multiplying each of its three numbers by an arbitrary number n. For example, from $(3,4,5)$ we get $(6,8,10)$, $(9,12,15)$, $(12,16,20)$, and so on. This process produces right triangles that are all similar to each other, so in a sense they are not essentially different triples. In our search for Pythagorean triples there is thus no harm in restricting our attention to triples (a,b,c) whose three numbers have no common factor. Such triples are called *primitive*. The large Babylonian triple mentioned above is primitive, since the prime factorization of 13500 is $2^2 3^3 5^3$ but the other two numbers in the triple are not divisible by 2, 3, or 5.

A fact worth noting in passing is that if two of the three numbers in a Pythagorean triple (a,b,c) have a common factor n, then n is also a factor of the third number. This follows easily from the equation $a^2+b^2=c^2$, since for example if n divides a and b then n^2 divides a^2 and b^2, so n^2 divides their sum c^2, hence n divides c. Another case is that n divides a and c. Then n^2 divides a^2 and c^2 so n^2 divides their difference $c^2-a^2=b^2$, hence n divides b. In the remaining case that n divides b and c the argument is similar.

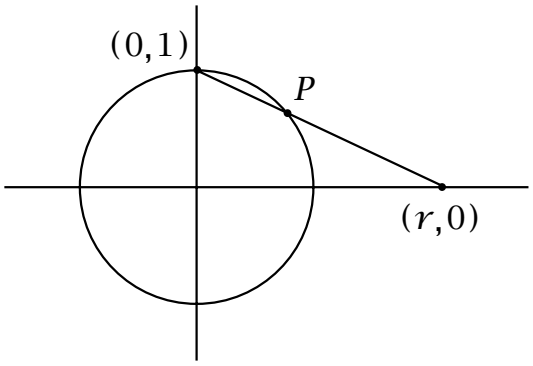
A consequence of this divisibility fact is that primitive Pythagorean triples can also be characterized as the ones for which no two of the three numbers have a common factor.

If (a,b,c) is a Pythagorean triple, then we can divide the equation $a^2+b^2=c^2$ by c^2 to get an equivalent equation $(\frac{a}{c})^2+(\frac{b}{c})^2=1$. This equation is saying that the point $(x,y)=(\frac{a}{c},\frac{b}{c})$ is on the unit circle $x^2+y^2=1$ in the xy-plane. The coordinates $\frac{a}{c}$ and $\frac{b}{c}$ are rational numbers, so each Pythagorean triple gives a *rational point* on the circle, i.e., a point whose coordinates are both rational. Notice that multiplying

each of a, b, and c by the same integer n yields the same point (x, y) on the circle. Going in the other direction, given a rational point on the circle, we can find a common denominator for its two coordinates so that it has the form $(\frac{a}{c}, \frac{b}{c})$ and hence gives a Pythagorean triple (a, b, c). We can assume this triple is primitive by canceling any common factor of a, b, and c, and this doesn't change the point $(\frac{a}{c}, \frac{b}{c})$. The two fractions $\frac{a}{c}$ and $\frac{b}{c}$ must then be in lowest terms since we observed earlier that if two of a, b, c have a common factor, then all three have a common factor.

From the preceding observations we can conclude that the problem of finding all Pythagorean triples is equivalent to finding all rational points on the unit circle $x^2 + y^2 = 1$. More specifically, there is an exact one-to-one correspondence between primitive Pythagorean triples and rational points on the unit circle that lie in the interior of the first quadrant (since we want all of a, b, c, x, y to be positive).

In order to find all the rational points on the circle $x^2 + y^2 = 1$ we will use a construction that starts with one rational point and creates many more rational points from this one starting point. The four obvious rational points on the circle are the intersections of the circle with the coordinate axes, which are the points $(\pm 1, 0)$ and $(0, \pm 1)$. It doesn't really matter which one we choose as the starting point, so let's choose $(0, 1)$. Now consider a line which intersects the circle in this point $(0, 1)$ and some other point P, as in the figure at the right. If the line has slope m, its equation will be $y = mx + 1$. If we denote the point where the line intersects the x-axis by $(r, 0)$, then $m = -1/r$ so the equation for the line can be rewritten as $y = 1 - \frac{x}{r}$. To find the coordinates of the point P in terms of r we substitute $y = 1 - \frac{x}{r}$ into the equation $x^2 + y^2 = 1$ and solve for x:



$$\begin{aligned}
x^2 + \left(1 - \frac{x}{r}\right)^2 &= 1 \\
x^2 + 1 - \frac{2x}{r} + \frac{x^2}{r^2} &= 1 \\
\left(1 + \frac{1}{r^2}\right)x^2 - \frac{2x}{r} &= 0 \\
\left(\frac{r^2+1}{r^2}\right)x^2 &= \frac{2x}{r} \\
x &= \frac{2r}{r^2+1} \quad \text{or} \quad x = 0
\end{aligned}$$

Now we plug $x = \dfrac{2r}{r^2+1}$ into the formula $y = 1 - \frac{x}{r}$. This gives:

$$y = 1 - \frac{x}{r} = -\frac{1}{r}\left(\frac{2r}{r^2+1}\right) + 1 = \frac{-2}{r^2+1} + 1 = \frac{r^2-1}{r^2+1}$$

Summarizing, the coordinates (x, y) of the point P are given by the following formula:

$$(x, y) = \left(\frac{2r}{r^2+1}, \frac{r^2-1}{r^2+1}\right)$$

Note that when $x = 0$ there are two points $(0, \pm 1)$ on the circle. The point $(0, -1)$ comes from the value $r = 0$, while if we let r approach $\pm\infty$ then the point P approaches $(0, 1)$, as we can see either from the picture or from the formula for (x, y).

If r is a rational number, then the formula for (x, y) shows that both x and y are rational, so we have a rational point on the circle. Conversely, if both coordinates x and y of the point P on the circle are rational, then the slope m of the line must be rational, hence r must also be rational since $r = -1/m$. We could also solve the equation $y = 1 - \frac{x}{r}$ for r to get $r = \frac{x}{1-y}$, showing again that r will be rational if x and y are rational (and y is not 1). The conclusion of all this is that, starting from the initial rational point $(0, 1)$ we have found formulas that give all the other rational points on the circle.

Since there are infinitely many choices for the rational number r, there are infinitely many rational points on the circle. But we can say something much stronger than this: Every arc of the circle, no matter how small, contains infinitely many rational points. This is because every arc on the circle corresponds to an interval of r-values on the x-axis, and every interval in the x-axis contains infinitely many rational numbers. Since every arc on the circle contains infinitely many rational points, we can say that the rational points are *dense* in the circle, meaning that for every point on the circle there is an infinite sequence of rational points approaching the given point.

Now we can go back and find formulas for Pythagorean triples. If we set the rational number r equal to p/q with p and q integers having no common factor, then the formulas for x and y become:

$$x = \frac{2(\frac{p}{q})}{\frac{p^2}{q^2}+1} = \frac{2pq}{p^2+q^2}$$

$$y = \frac{\frac{p^2}{q^2}-1}{\frac{p^2}{q^2}+1} = \frac{p^2-q^2}{p^2+q^2}$$

Our final formulas for Pythagorean triples are then:

$$(a, b, c) = (2pq, p^2-q^2, p^2+q^2)$$

Here are a few examples with small values of p and q:

(p,q)	(x,y)	(a,b,c)
$(2,1)$	$(4/5,3/5)$	$(4,3,5)$
$(3,1)^*$	$(6/10,8/10)^*$	$(6,8,10)^*$
$(3,2)$	$(12/13,5/13)$	$(12,5,13)$
$(4,1)$	$(8/17,15/17)$	$(8,15,17)$
$(4,3)$	$(24/25,7/25)$	$(24,7,25)$
$(5,1)^*$	$(10/26,24/26)^*$	$(10,24,26)^*$
$(5,2)$	$(20/29,21/29)$	$(20,21,29)$
$(5,3)^*$	$(30/34,16/34)^*$	$(30,16,34)^*$
$(5,4)$	$(40/41,9/41)$	$(40,9,41)$
$(6,1)$	$(12/37,35/37)$	$(12,35,37)$
$(6,5)$	$(60/61,11/61)$	$(60,11,61)$
$(7,1)^*$	$(14/50,48/50)^*$	$(14,48,50)^*$
$(7,2)$	$(28/53,45/53)$	$(28,45,53)$
$(7,3)^*$	$(42/58,40/58)^*$	$(42,40,58)^*$
$(7,4)$	$(56/65,33/65)$	$(56,33,65)$
$(7,5)^*$	$(70/74,24/74)^*$	$(70,24,74)^*$
$(7,6)$	$(84/85,13/85)$	$(84,13,85)$

The starred entries are the ones with nonprimitive Pythagorean triples. Notice that this occurs only when p and q are both odd, so that not only is $2pq$ even, but also both p^2-q^2 and p^2+q^2 are even, so all three of a, b, and c are divisible by 2. The primitive versions of the nonprimitive entries in the table occur higher in the table, but with a and b switched. This is a general phenomenon, as we will see in the course of proving the following basic result:

Proposition. *Up to interchanging a and b, all primitive Pythagorean triples (a,b,c) are obtained from the formula $(a,b,c) = (2pq, p^2-q^2, p^2+q^2)$ where p and q are positive integers, $p>q$, such that p and q have no common factor and are of opposite parity (one even and the other odd).*

Proof: We need to investigate when the formula $(a,b,c) = (2pq, p^2-q^2, p^2+q^2)$ gives a primitive triple, assuming that p and q have no common divisor and $p>q$.

Case 1: Suppose p and q have opposite parity. If all three of $2pq$, p^2-q^2, and p^2+q^2 have a common divisor $d>1$ then d would have to be odd since p^2-q^2 and p^2+q^2 are odd when p and q have opposite parity. Furthermore, since d is a divisor of both p^2-q^2 and p^2+q^2 it must divide their sum $(p^2+q^2)+(p^2-q^2)=2p^2$ and also their difference $(p^2+q^2)-(p^2-q^2)=2q^2$. However, since d is odd it would then have to divide p^2 and q^2, forcing p and q to have a common factor (since any prime factor of d would have to divide p and q). This contradicts the assumption that p and q had no common factors, so we conclude that $(2pq, p^2-q^2, p^2+q^2)$ is primitive if p and q have opposite parity.

Case 2: Suppose p and q have the same parity, hence they are both odd since if they were both even they would have the common factor of 2. Because p and q are both odd, their sum and difference are both even and we can write $p+q=2P$ and

$p-q=2Q$ for some integers P and Q. Any common factor of P and Q would have to divide $P+Q=\frac{p+q}{2}+\frac{p-q}{2}=p$ and $P-Q=\frac{p+q}{2}-\frac{p-q}{2}=q$, so P and Q have no common factors. In terms of P and Q our Pythagorean triple becomes

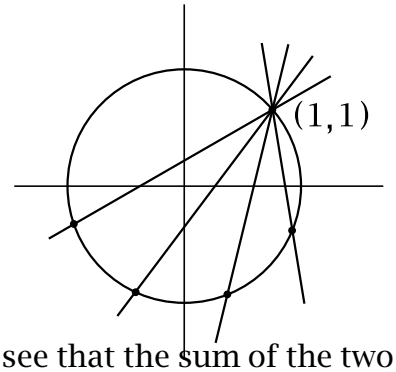
$$\begin{aligned}(a,b,c)&=(2pq,p^2-q^2,p^2+q^2)\\&=(2(P+Q)(P-Q),(P+Q)^2-(P-Q)^2,(P+Q)^2+(P-Q)^2)\\&=(2(P^2-Q^2),4PQ,2(P^2+Q^2))\\&=2(P^2-Q^2,2PQ,P^2+Q^2)\end{aligned}$$

After canceling the factor of 2 we get a new Pythagorean triple, with the first two coordinates switched, and this one is primitive by Case 1 since P and Q can't both be odd, because if they were, then $p=P+Q$ and $q=P-Q$ would both be even, which is impossible since they have no common factor.

From Cases 1 and 2 we can conclude that if we allow ourselves to switch the first two coordinates, then we get all primitive Pythagorean triples from the formula by restricting p and q to be of opposite parity and to have no common factors. □

Rational Points on Other Quadratic Curves

The same technique we used to find the rational points on the circle $x^2+y^2=1$ can also be used to find all the rational points on other quadratic curves $Ax^2+Bxy+Cy^2+Dx+Ey=F$ with integer or rational coefficients A, B, C, D, E, F, provided that we can find a single rational point (x_0,y_0) on the curve to start the process. For example, the circle $x^2+y^2=2$ contains the rational points $(\pm1,\pm1)$ and we can use one of these as an initial point. Taking the point $(1,1)$, we would consider lines $y-1=m(x-1)$ of slope m passing through this point. Solving this equation for y and plugging into the equation $x^2+y^2=2$ would produce a quadratic equation $ax^2+bx+c=0$ whose coefficients are polynomials in the variable m, so these coefficients would be rational whenever m is rational.



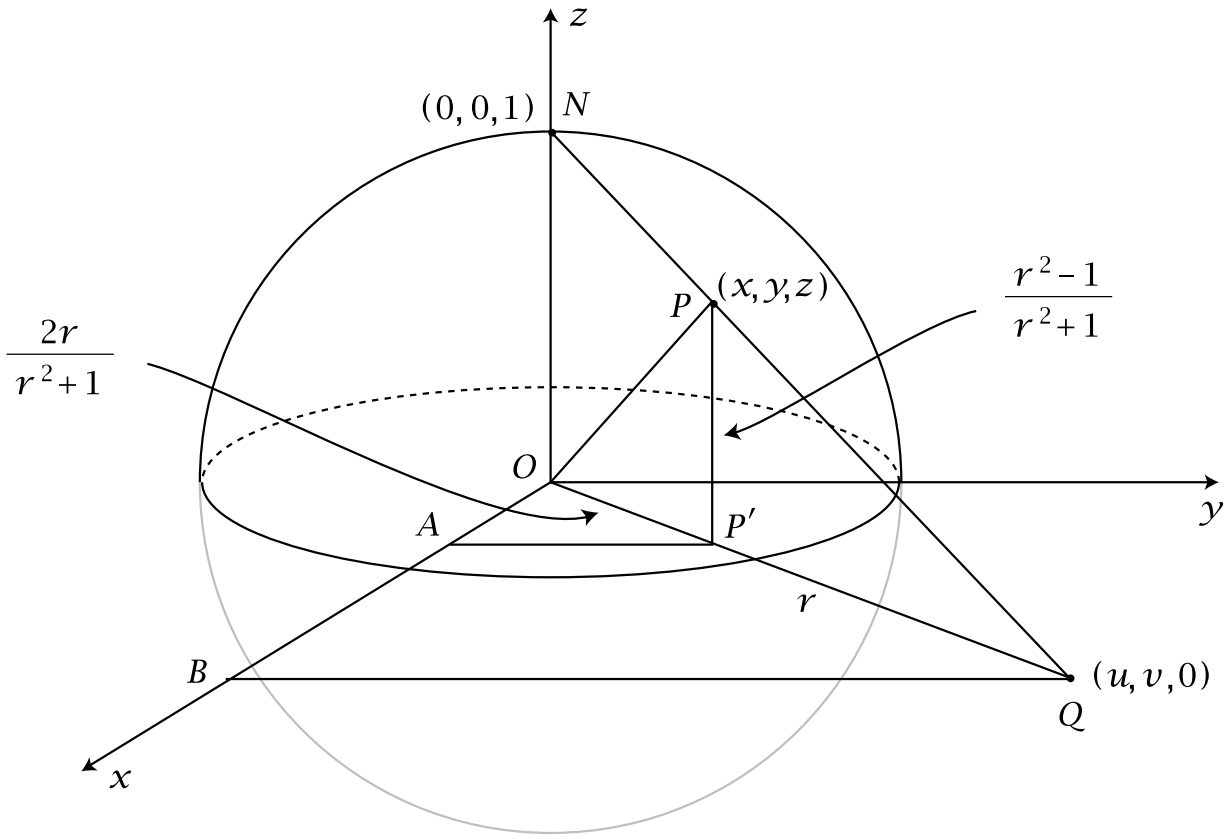
From the quadratic formula $x=(-b\pm\sqrt{b^2-4ac})/2a$ we see that the sum of the two roots is $-b/a$, a rational number if m is rational, so if one root is rational then the other root will be rational as well. The initial point $(1,1)$ on the curve $x^2+y^2=2$ gives $x=1$ as one rational root of the equation $ax^2+bx+c=0$, so for each rational value of m the other root x will be rational as well. Then the equation $y-1=m(x-1)$ implies that y will also be rational, and hence we obtain a rational point (x,y) on the curve for each rational value of m. Conversely, if x and y are both rational then obviously $m=(y-1)/(x-1)$ will be rational. Thus one obtains a dense set of rational points on the circle $x^2+y^2=2$, since m can be any rational number. An exercise at the end of this chapter is to work out the formulas explicitly.

If instead of $x^2 + y^2 = 2$ we consider the circle $x^2 + y^2 = 3$ then there aren't any obvious rational points. In fact this circle contains no rational points at all. For if there were a rational point, this would yield a solution of the equation $a^2 + b^2 = 3c^2$ by integers a, b, and c. We can assume a, b, and c have no common factor. Then a and b can't both be even, otherwise the left side of the equation would be even, forcing c to be even, so a, b, and c would have a common factor of 2. To complete the argument we look at the equation modulo 4. (This means that we consider the remainders obtained after division by 4.) The square of an even number has the form $(2n)^2 = 4n^2$, which is 0 modulo 4, while the square of an odd number has the form $(2n + 1)^2 = 4n^2 + 4n + 1$, which is 1 modulo 4. Thus, modulo 4, the left side of the equation is either $0 + 1$, $1 + 0$, or $1 + 1$ since a and b are not both even. So the left side is either 1 or 2 modulo 4. However, the right side is either $3 \cdot 0$ or $3 \cdot 1$ modulo 4. We conclude that there can be no integer solutions of $a^2 + b^2 = 3c^2$.

The technique we just used to show that $a^2 + b^2 = 3c^2$ has no integer solutions can be used in many other situations as well. The underlying reasoning is that if an equation with integer coefficients has an integer solution, then this gives a solution modulo n for all numbers n. For solutions modulo n there are only a finite number of possibilities to check, although for large n this is a large finite number. If one can find a single value of n for which there is no solution modulo n, then the original equation has no integer solutions. However, this implication is not reversible, as it is possible for an equation to have solutions modulo n for every number n and still have no actual integer solutions. A concrete example is the equation $2x^2 + 7y^2 = 1$. This obviously has no integer solutions, yet it does have solutions modulo n for each n, although this is certainly not obvious and proving it would require developing some general theory first. Note that the ellipse $2x^2 + 7y^2 = 1$ does contain rational points such as $(1/3, 1/3)$ and $(3/5, 1/5)$. These can in fact be used to show that $2x^2 + 7y^2 = 1$ has solutions modulo n for each n.

Rational Points on a Sphere

As another application of the same idea, we can find all the rational points on the sphere $x^2 + y^2 + z^2 = 1$, the triples (x, y, z) of rational numbers that satisfy this equation. To do this we consider a line from the north pole $(0, 0, 1)$ to a point $(u, v, 0)$ in the xy-plane. This line intersects the sphere at some point (x, y, z). We want to find formulas expressing x, y, and z in terms of u and v.



Suppose we look at the vertical plane containing the triangle ONQ. From our earlier analysis of rational points on a circle of radius 1 we know that if the segment OQ has length $|OQ| = r$, then $|OP'| = \frac{2r}{r^2+1}$ and $|PP'| = \frac{r^2-1}{r^2+1}$. From the right triangle OBQ we see that $u^2 + v^2 = r^2$ since $u = |OB|$ and $v = |BQ|$. The triangle OBQ is similar to the triangle OAP'. Since the length of OP' is $\frac{2}{r^2+1}$ times the length of OQ we conclude from similar triangles that

$$x = |OA| = \frac{2}{r^2+1}|OB| = \frac{2}{r^2+1} \cdot u = \frac{2u}{u^2+v^2+1}$$

and

$$y = |AP'| = \frac{2}{r^2+1}|BQ| = \frac{2}{r^2+1} \cdot v = \frac{2v}{u^2+v^2+1}$$

Also we have

$$z = |PP'| = \frac{r^2-1}{r^2+1} = \frac{u^2+v^2-1}{u^2+v^2+1}$$

Summarizing, we have expressed x, y, and z in terms of u and v by the formulas

$$x = \frac{2u}{u^2+v^2+1} \qquad y = \frac{2v}{u^2+v^2+1} \qquad z = \frac{u^2+v^2-1}{u^2+v^2+1}$$

These formulas imply that we get a rational point (x, y, z) on the sphere $x^2+y^2+z^2 = 1$ for each pair of rational numbers (u, v). We get all rational points on the sphere in this way (except for the north pole $(0, 0, 1)$, of course) since it is possible to express u and v in terms of x, y, and z by the formulas

$$u = \frac{x}{1-z} \qquad v = \frac{y}{1-z}$$

which one can easily verify by substituting into the previous formulas.

Here is a short table giving a few rational points on the sphere and the corresponding integer solutions of the equation $a^2 + b^2 + c^2 = d^2$:

(u, v)	(x, y, z)	(a, b, c, d)
$(1, 1)$	$(2/3, 2/3, 1/3)$	$(2, 2, 1, 3)$
$(2, 2)$	$(4/9, 4/9, 7/9)$	$(4, 4, 7, 9)$
$(1, 3)$	$(2/11, 6/11, 9/11)$	$(2, 6, 9, 11)$
$(2, 3)$	$(2/7, 3/7, 6/7)$	$(2, 3, 6, 7)$
$(1, 4)$	$(1/9, 4/9, 8/9)$	$(1, 4, 8, 9)$

As with rational points on the circle $x^2 + y^2 = 1$, rational points on the sphere $x^2 + y^2 + z^2 = 1$ are dense, so there are lots of them all over on the sphere.

In linear algebra courses one is often called upon to create unit vectors (x, y, z) by taking a given vector and rescaling to have length 1 by dividing it by its length. For example, the vector $(1, 1, 1)$ has length $\sqrt{3}$ so the corresponding unit vector is $(1/\sqrt{3}, 1/\sqrt{3}, 1/\sqrt{3})$. It is rare that this process produces unit vectors having rational coordinates, but we now have a method for creating as many rational unit vectors as we like.

Incidentally, there is a name for the correspondence we have described between points (x, y, z) on the unit sphere and points (u, v) in the plane: it is called *stereographic projection*. One can think of the sphere and the plane as being made of clear glass, and one puts one's eye at the north pole of the sphere and looks downward and outward in all directions to see points on the sphere projected onto points in the plane, and vice versa. The north pole itself does not project onto any point in the plane, but points approaching the north pole project to points approach infinity in the plane, so one can think of the north pole as corresponding to an imaginary infinitely distant "point" in the plane. This geometric viewpoint somehow makes infinity less of a mystery, as it just corresponds to a point on the sphere, and points on a sphere are not very mysterious. (Though in the early days of polar exploration the north pole may have seemed very mysterious and infinitely distant!)

Pythagorean Triples and Quadratic Forms

There are many questions one can ask about Pythagorean triples (a,b,c). For example, we could begin by asking which numbers actually arise as the numbers a, b, or c in some Pythagorean triple. It is sufficient to answer the question just for primitive Pythagorean triples, since the remaining ones are obtained just by multiplying by arbitrary positive integers. We know all primitive Pythagorean triples arise from the formula

$$(a,b,c) = (2pq, p^2-q^2, p^2+q^2)$$

where p and q have no common factor and are not both odd. Determining whether a given number can be expressed in the form $2pq$, p^2-q^2, or p^2+q^2 is a special case of the general question of deciding when an equation $Ap^2+Bpq+Cq^2=n$ has an integer solution p, q, for given integers A, B, C, and n. Expressions of the form $Ax^2+Bxy+Cy^2$ are called *quadratic forms*. These will be the main topic studied in Chapters 4–6, where we will develop some general theory addressing the question of what values a quadratic form takes on when all the numbers involved are integers. For now, let us just look at the special cases at hand.

First let us consider which numbers occur as a or b in Pythagorean triples (a,b,c). We certainly can't realize the number 1 since this would say $a^2+1=c^2$ or $1+b^2=c^2$ but 1 is not the difference between the squares of any two positive integers. For numbers bigger than 1, if we look at the earlier table of Pythagorean triples we see that all the numbers up to 15 can be realized as a or b in primitive triples except for 2, 6, 10, and 14. This might lead us to guess that the numbers realizable as a or b in primitive triples are the numbers not congruent to 2 modulo 4. This is indeed true, and can be proved as follows. First note that $2pq$ is even and p^2-q^2 is odd (otherwise both a and b would be even, violating primitivity). Every odd number bigger than 1 is expressible in the form p^2-q^2 since $2k+1=(k+1)^2-k^2$, so in fact every odd number is the difference between two consecutive squares. Note that taking $p=k+1$ and $q=k$ does yield a primitive triple since k and $k+1$ always have opposite parity and no common factors. This takes care of realizing odd numbers. For even numbers, they would have to be of the form $2pq$, and by taking $q=1$ we realize any even number $2p$. However, to have a primitive triple we have to have p even since p must have opposite parity from q which is 1. Thus we realize the numbers $a=4k$ by primitive triples but not the numbers $a=4k+2$. This is what we claimed was true. To finish the story for a and b, note that a number $a=4k+2$ which can't be realized by a primitive triple can be realized by a nonprimitive triple, at least if $k\ge 1$, since we know we can realize the odd number $2k+1$ if $k\ge 1$, and by doubling this we realize $4k+2$. Summarizing this discussion, all numbers greater than 2 can be realized as a or b in Pythagorean triples (a,b,c).

Now let us ask which numbers c can occur in Pythagorean triples (a,b,c), so we are trying to find a solution of $p^2+q^2=c$ for a given number c. Pythagorean triples

(p,q,r) give solutions when c is equal to a square r^2, but we are asking now about arbitrary numbers c. It suffices to figure out which numbers c occur in primitive triples (a,b,c), since by multiplying the numbers c in primitive triples by arbitrary numbers we get the numbers c in arbitrary triples. A look at the earlier table shows that the numbers c that can be realized by primitive triples (a,b,c) seem to be fairly rare: only 5, 13, 17, 25, 29, 37, 41, 53, 61, 65, and 85 occur in the table. These are all odd, and in fact they are all congruent to 1 modulo 4. This always has to be true because p and q are of opposite parity, so one of p^2 and q^2 is congruent to 0 modulo 4 while the other is congruent to 1, hence p^2+q^2 is congruent to 1 modulo 4. More interesting is the fact that most of the numbers on the list are prime numbers, and the ones that aren't prime are products of earlier primes in the list: $25 = 5\cdot 5$, $65 = 5\cdot 13$, $85 = 5\cdot 17$. From this somewhat slim evidence one might conjecture that the numbers c occurring in primitive Pythagorean triples are exactly the numbers that are products of primes congruent to 1 modulo 4. The first prime satisfying this condition that isn't on the original list is 73, and this is realized as $p^2+q^2 = 8^2+3^2$, in the triple $(48,55,73)$. The next two primes congruent to 1 modulo 4 are $89 = 8^2+5^2$ and $97 = 9^2+4^2$, so the conjecture continues to look good. Proving the general conjecture is not easy, however, and we will take up this question in Chapter 6 when we fully answer the question of which numbers can be expressed as the sum of two squares.

Another question one can ask about Pythagorean triples is, how many are there where two of the three numbers differ by only 1? In the earlier table there are several: $(3,4,5)$, $(5,12,13)$, $(7,24,25)$, $(20,21,29)$, $(9,40,41)$, $(11,60,61)$, and $(13,84,85)$. As the pairs of numbers that are adjacent get larger, the corresponding right triangles are either approximately 45-45-90 right triangles as with the triple $(20,21,29)$, or long thin triangles as with $(13,84,85)$. To analyze the possibilities, note first that if two of the numbers in a triple (a,b,c) differ by 1 then the triple has to be primitive, so we can use our formula $(a,b,c) = (2pq, p^2-q^2, p^2+q^2)$. If b and c differ by 1 then we would have $(p^2+q^2)-(p^2-q^2) = 2q^2 = 1$ which is impossible. If a and c differ by 1 then we have $p^2+q^2-2pq = (p-q)^2 = 1$ so $p-q = \pm 1$, and in fact $p-q = +1$ since we have to have $p>q$ in order for $b = p^2-q^2$ to be positive. Thus we get the infinite sequence of solutions $(p,q) = (2,1),(3,2),(4,3),\cdots$ with corresponding triples $(4,3,5),(12,5,13),(24,7,25),\cdots$. Note that these are the same triples we obtained earlier that realize all the odd values $b = 3,5,7,\cdots$.

The remaining case is that a and b differ by 1. Thus we have the equation $p^2-2pq-q^2 = \pm 1$. The left side doesn't factor using integer coefficients, so it's not so easy to find integer solutions this time. In the table there are only the two triples $(4,3,5)$ and $(20,21,29)$, with $(p,q) = (2,1)$ and $(5,2)$. After some trial and error one could find the next solution $(p,q) = (12,5)$ which gives the triple $(120,119,169)$. Is there a pattern in the solutions $(2,1),(5,2),(12,5)$? One has the numbers $1,2,5,12$,

and perhaps it isn't too much of a stretch to notice that the third number is twice the second plus the first, while the fourth number is twice the third plus the second. If this pattern continued, the next number would be $29 = 2 \cdot 12 + 5$, giving $(p,q) = (29,12)$, and this does indeed satisfy $p^2 - 2pq - q^2 = 1$, yielding the Pythagorean triple $(696,697,985)$. These numbers are increasing rather rapidly, and the next case $(p,q) = (70,29)$ yields an even bigger Pythagorean triple $(4060,4059,5741)$. Could there be other solutions of $p^2 - 2pq - q^2 = \pm 1$ with smaller numbers that we missed? We will develop tools in Chapters 4 and 5 to find all the integer solutions, and it will turn out that the sequence we have just discovered gives them all.

Although the quadratic form $p^2 - 2pq - q^2$ does not factor using integer coefficients, it can be simplified slightly be rewriting it as $(p-q)^2 - 2q^2$. Then if we change variables by setting

$$x = p - q$$

$$y = q$$

we obtain the quadratic form $x^2 - 2y^2$. Finding integer solutions of $x^2 - 2y^2 = n$ is equivalent to finding integer solutions of $p^2 - 2pq - q^2 = n$ since integer values of p and q give integer values of x and y, and conversely, integer values of x and y give integer values of p and q since when we solve for p and q in terms of x and y we again get equations with integer coefficients:

$$p = x + y$$

$$q = y$$

Thus the quadratic forms $p^2 - 2pq - q^2$ and $x^2 - 2y^2$ are completely equivalent, and finding integer solutions of $p^2 - 2pq - q^2 = \pm 1$ is equivalent to finding integer solutions of $x^2 - 2y^2 = \pm 1$.

The equation $x^2 - 2y^2 = \pm 1$ is an instance of the equation $x^2 - Dy^2 = \pm 1$ which is known as *Pell's equation*. This is a very famous equation in number theory which has arisen in many different contexts going back hundreds of years. We will develop techniques for finding all integer solutions of Pell's equation for arbitrary values of D in Chapters 4 and 5. It is interesting that certain fairly small values of D can force the solutions to be quite large. For example for $D = 61$ the smallest positive integer solution of $x^2 - 61y^2 = 1$ is the rather large pair

$$(x,y) = (1766319049, 226153980)$$

As far back as the eleventh and twelfth centuries mathematicians in India knew how to find this solution. It was rediscovered in the seventeenth century by Fermat in France, who also gave the smallest solution of $x^2 - 109y^2 = 1$, the even larger pair

$$(x,y) = (158070671986249, 15140424455100)$$

The way that the size of the smallest solution of $x^2 - Dy^2 = 1$ depends upon D is very erratic and is still not well understood today.

Pythagorean Triples and Complex Numbers

There is another way of looking at Pythagorean triples that involves complex numbers, surprisingly enough. The starting point here is the observation that a^2+b^2 can be factored as $(a+bi)(a-bi)$ where $i=\sqrt{-1}$. If we rewrite the equation $a^2+b^2=c^2$ as $(a+bi)(a-bi)=c^2$ then since the right side of the equation is a square, we might wonder whether each term on the left side would have to be a square too. For example, in the case of the triple $(3,4,5)$ we have $(3+4i)(3-4i)=5^2$ with $3+4i=(2+i)^2$ and $3-4i=(2-i)^2$. So let us ask optimistically whether the equation $(a+bi)(a-bi)=c^2$ can be rewritten as $(p+qi)^2(p-qi)^2=c^2$ with $a+bi=(p+qi)^2$ and $a-bi=(p-qi)^2$. We might hope also that the equation $(p+qi)^2(p-qi)^2=c^2$ was obtained by simply squaring the equation $(p+qi)(p-qi)=c$. Let us see what happens when we multiply these various products out:

$$\begin{aligned} a+bi=(p+qi)^2&=(p^2-q^2)+(2pq)i\\ &\text{hence}\quad a=p^2-q^2\quad\text{and}\quad b=2pq\\ a-bi=(p-qi)^2&=(p^2-q^2)-(2pq)i\\ &\text{hence again}\quad a=p^2-q^2\quad\text{and}\quad b=2pq\\ c=(p+qi)(p-qi)&=p^2+q^2 \end{aligned}$$

Thus we have miraculously recovered the formulas for Pythagorean triples that we obtained earlier by geometric means (with a and b switched, which doesn't really matter):

$$a=p^2-q^2 \qquad b=2pq \qquad c=p^2+q^2$$

Of course, our derivation of these formulas just now depended on several assumptions that we haven't justified, but it does suggest that looking at complex numbers of the form $a+bi$ where a and b are integers might be a good idea. There is a name for complex numbers of this form $a+bi$ with a and b integers. They are called *Gaussian integers*, since the great mathematician and physicist C.F.Gauss made a thorough algebraic study of them some 200 years ago. We will develop the basic properties of Gaussian integers in Chapter 7, in particular explaining why the derivation of the formulas above is valid.

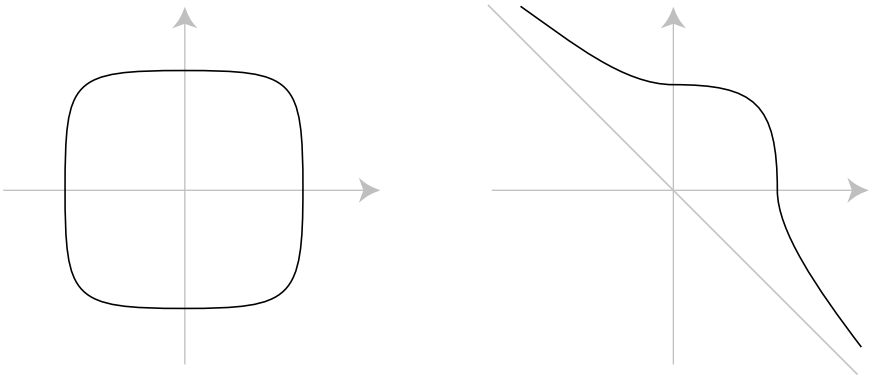
Diophantine Equations

Equations like $x^2+y^2=z^2$ or $x^2-Dy^2=1$ that involve polynomials with integer coefficients, and where the solutions sought are required to be integers, are called *Diophantine equations* after the Greek mathematician Diophantus (ca. 250 A.D.) who wrote a book about these equations that was very influential when European mathematicians started to consider this topic much later in the 1600s. Usually Diophantine equations are very hard to solve because of the restriction to integer solutions. The first really interesting case is quadratic Diophantine equations. By the year 1800 there

was quite a lot known about the quadratic case, and we will be focusing on this case in this book.

Diophantine equations of higher degree than quadratic are much more challenging to understand. Probably the most famous one is $x^n + y^n = z^n$ where n is a fixed integer greater than 2. When the French mathematician Fermat in the 1600s was reading about Pythagorean triples in his copy of Diophantus' book he made a marginal note that, in contrast with the equation $x^2 + y^2 = z^2$, the equation $x^n + y^n = z^n$ has no solutions with positive integers x, y, z when $n > 2$ and that he had a marvelous proof which unfortunately the margin was too narrow to contain. This is one of many statements that he claimed were true but never wrote proofs of for public distribution, nor have proofs been found among his manuscripts. Over the next century other mathematicians discovered proofs for all his other statements, but this one was far more difficult to verify. The issue is clouded by the fact that he only wrote this statement down the one time, whereas all his other important results were stated numerous times in his correspondence with other mathematicians of the time. So perhaps he only briefly believed he had a proof. In any case, the statement has become known as Fermat's Last Theorem. It was finally proved in the 1990s by Andrew Wiles, using some very deep mathematics developed over the preceding couple decades.

Just as finding integer solutions of $x^2 + y^2 = z^2$ is equivalent to finding rational points on the circle $x^2 + y^2 = 1$, so finding integer solutions of $x^n + y^n = z^n$ is equivalent to finding rational points on the curve $x^n + y^n = 1$. For even values of $n > 2$ this curve looks like a flattened out circle while for odd n it has a rather different shape, extending out to infinity in the second and fourth quadrants, asymptotic to the line $y = -x$:



Fermat's Last Theorem is equivalent to the statement that these curves have no rational points except their intersections with the coordinate axes, where either x or y is 0. It is curious that these curves only contain a finite number of rational points (either two points or four points, depending on whether n odd or even) whereas quadratic curves like $x^2 + y^2 = n$ either contain no rational points or an infinite dense set of rational points.

Exercises

1. (a) Make a list of the 16 primitive Pythagorean triples (a,b,c) with $c \le 100$, regarding (a,b,c) and (b,a,c) as the same triple.
(b) How many more would there be if we allowed nonprimitive triples?
(c) How many triples (primitive or not) are there with $c = 65$?

2. (a) Find all the positive integer solutions of $x^2 - y^2 = 512$ by factoring $x^2 - y^2$ as $(x+y)(x-y)$ and considering the possible factorizations of 512.
(b) Show that the equation $x^2 - y^2 = n$ has only a finite number of integer solutions for each value of $n > 0$.
(c) Find a value of $n > 0$ for which the equation $x^2 - y^2 = n$ has at least 100 different positive integer solutions.

3. (a) Show that there are only a finite number of Pythagorean triples (a,b,c) with a equal to a given number n.
(b) Show that there are only a finite number of Pythagorean triples (a,b,c) with c equal to a given number n.

4. Find an infinite sequence of primitive Pythagorean triples where two of the numbers in each triple differ by 2.

5. Find a right triangle whose sides have integer lengths and whose acute angles are close to 30 and 60 degrees by first finding the irrational value of r that corresponds to a right triangle with acute angles exactly 30 and 60 degrees, then choosing a rational number close to this irrational value of r.

6. Find a right triangle whose sides have integer lengths and where one of the nonhypotenuse sides is approximately twice as long as the other, using a method like the one in the preceding problem. (One possible answer might be the $(8,15,17)$ triangle, or a triangle similar to this, but you should do better than this.)

7. Find a rational point on the sphere $x^2+y^2+z^2 = 1$ whose x, y, and z coordinates are nearly equal.

8. (a) Derive formulas that give all the rational points on the circle $x^2 + y^2 = 2$ in terms of a rational parameter m, the slope of the line through the point $(1,1)$ on the circle. (The value $m = \infty$ should be allowed as well, yielding the point $(1,-1)$.) The calculations may be a little messy, but they work out fairly nicely in the end to give

$$x = \frac{m^2 - 2m - 1}{m^2 + 1}, \qquad y = \frac{-m^2 - 2m + 1}{m^2 + 1}$$

(b) Using these formulas, find five different rational points on the circle in the first quadrant, and hence five solutions of $a^2 + b^2 = 2c^2$ with positive integers a, b, c.
(c) The equation $a^2 + b^2 = 2c^2$ can be rewritten as $c^2 = (a^2 + b^2)/2$, which says that c^2 is the average of a^2 and b^2, or in other words, the squares a^2, c^2, b^2 form an arithmetic progression. One can assume $a < b$ by switching a and b if necessary.

Find four such arithmetic progressions of three increasing squares where in each case the three numbers have no common divisors.

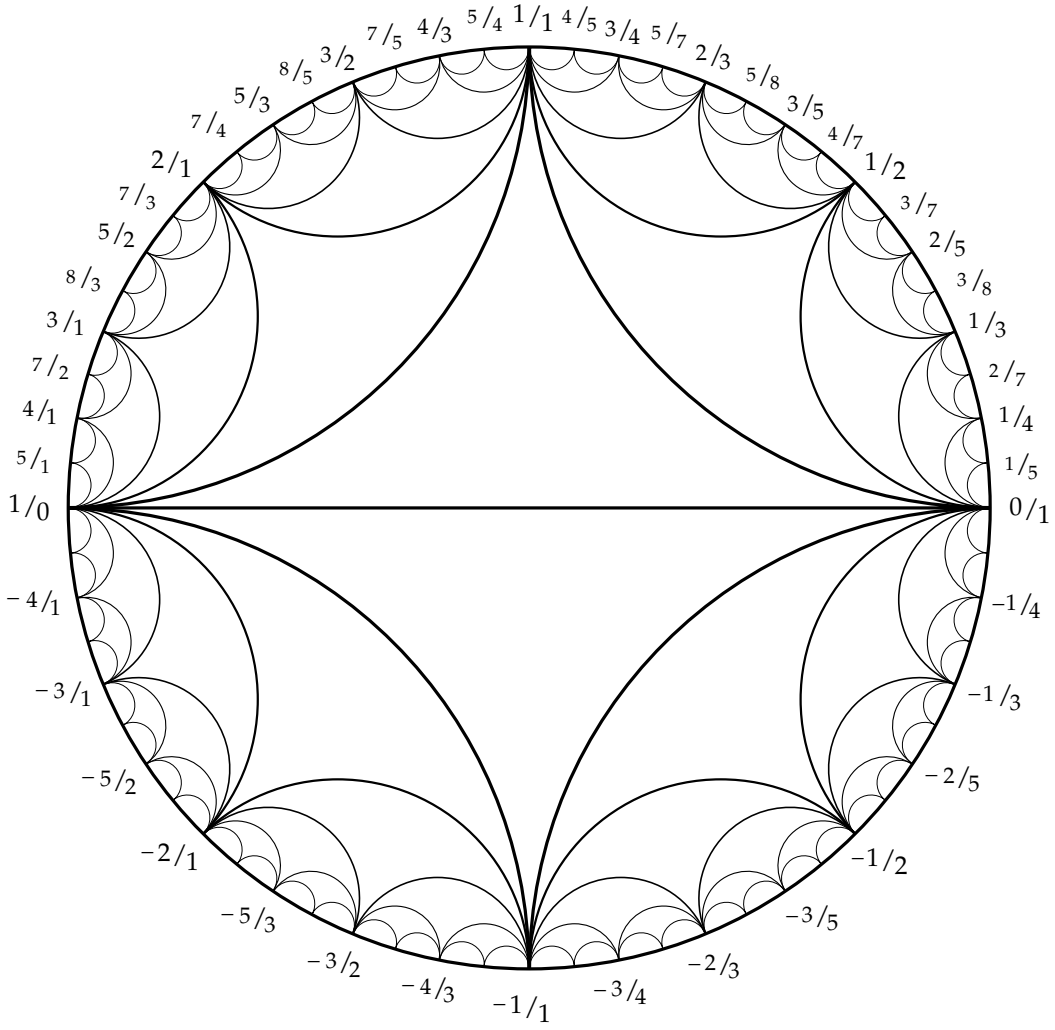
9. (a) Find formulas that give all the rational points on the upper branch of the hyperbola $y^2 - x^2 = 1$.
(b) Can you find any relationship between these rational points and Pythagorean triples?

10. (a) For integers x, what are the possible values of x^2 modulo 8?
(b) Show that the equation $x^2 - 2y^2 = \pm 3$ has no integer solutions by considering this equation modulo 8.
(c) Show that there are no primitive Pythagorean triples (a, b, c) with a and b differing by 3.

11. Show that for every Pythagorean triple (a, b, c) the product abc must be divisible by 60. (It suffices to show that abc is divisible by 3, 4, and 5.)

Chapter 1. The Farey Diagram

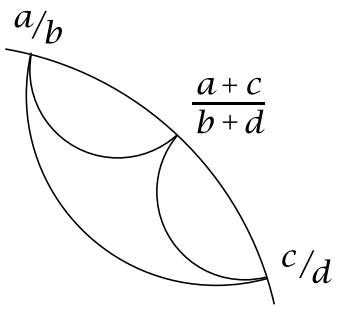
Our goal is to use geometry to study numbers. Of the various kinds of numbers, the simplest are integers, along with their ratios, the rational numbers. The large figure below shows a very interesting diagram displaying rational numbers and certain relations between them that we will be exploring. This diagram, along with several variants of it that will be introduced later, is known as the *Farey diagram*. The origin of the name will be explained when we get to one of these variants.



What is shown here is not the whole diagram but only a finite part of it. The actual diagram has infinitely many curvilinear triangles, getting smaller and smaller out near the boundary circle. The diagram can be constructed by first inscribing the two big triangles in the circle, then adding the four triangles that share an edge with the two big triangles, then the eight triangles sharing an edge with these four, then sixteen more triangles, and so on forever. With a little practice one can draw the diagram without lifting one's pencil from the paper: First draw the outer circle starting at the left or right side, then the diameter, then make the two large triangles, then the four next-largest triangles, etc.

The vertices of all the triangles are labeled with fractions a/b, including the

fraction $1/0$ for ∞, according to the following scheme. In the upper half of the diagram first label the vertices of the big triangles $0/1$, $1/1$, and $1/0$ as shown. Then by induction, if the labels at the two ends of the long edge of a triangle are a/b and c/d, the label on the third vertex of the triangle is $\frac{a+c}{b+d}$. This fraction is called the *mediant* of a/b and c/d.



The labels in the lower half of the diagram follow the same scheme, starting with the labels $0/1$, $-1/1$, and $-1/0$ on the large triangle. Using $-1/0$ instead of $1/0$ as the label of the vertex at the far left means that we are regarding $+\infty$ and $-\infty$ as the same. The labels in the lower half of the diagram are the negatives of those in the upper half, and the labels in the left half are the reciprocals of those in the right half.

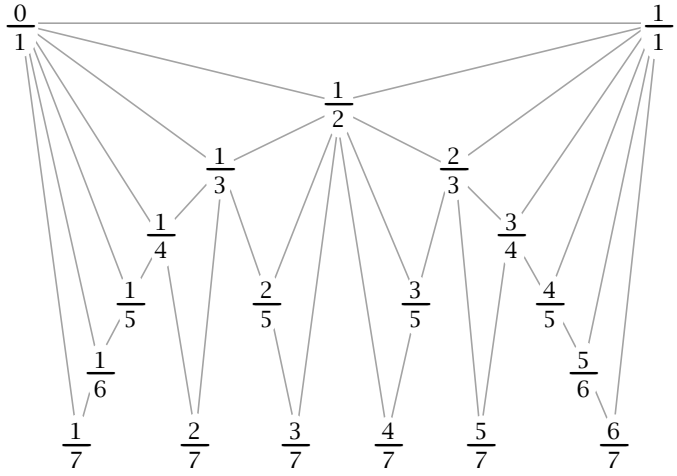
The labels occur in their proper order around the circle, increasing from $-\infty$ to $+\infty$ as one goes around the circle in the counterclockwise direction. To see why this is so, it suffices to look at the upper half of the diagram where all numbers are positive. What we want to show is that the mediant $\frac{a+c}{b+d}$ is always a number between $\frac{a}{b}$ and $\frac{c}{d}$ (hence the term "mediant"). Thus we want to see that if $\frac{a}{b} > \frac{c}{d}$ then $\frac{a}{b} > \frac{a+c}{b+d} > \frac{c}{d}$. Since we are dealing with positive numbers, the inequality $\frac{a}{b} > \frac{c}{d}$ is equivalent to $ad > bc$, and $\frac{a}{b} > \frac{a+c}{b+d}$ is equivalent to $ab + ad > ab + bc$ which follows from $ad > bc$. Similarly, $\frac{a+c}{b+d} > \frac{c}{d}$ is equivalent to $ad + cd > bc + cd$ which also follows from $ad > bc$.

We will show in the next chapter that the mediant rule for labeling vertices in the diagram automatically produces labels that are fractions in lowest terms. It is not immediately apparent why this should be so. For example, the mediant of $1/3$ and $2/3$ is $3/6$, which is not in lowest terms, and the mediant of $2/7$ and $3/8$ is $5/15$, again not in lowest terms. Somehow cases like this don't occur in the diagram.

Another non-obvious fact about the diagram is that all rational numbers occur eventually as labels of vertices. This will be shown in the next chapter as well.

Farey Series

We can build the set of rational numbers by starting with the integers and then inserting in succession all the halves, thirds, fourths, fifths, sixths, and so on. Let us look at what happens if we restrict to rational numbers between 0 and 1. Starting with 0 and 1 we first insert $1/2$, then $1/3$ and $2/3$, then $1/4$ and $3/4$, skipping $2/4$ which we already have, then inserting $1/5$, $2/5$, $3/5$, and $4/5$, then $1/6$ and $5/6$, etc. This process can be pictured as in the following diagram:



The interesting thing to notice is:

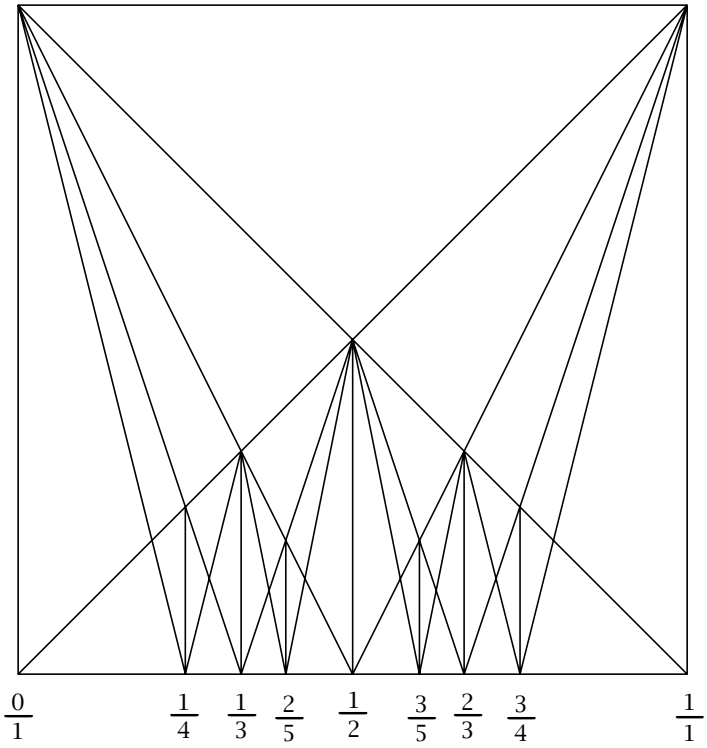
> *Each time a new number is inserted, it forms the third vertex of a triangle whose other two vertices are its two nearest neighbors among the numbers already listed, and if these two neighbors are a/b and c/d then the new vertex is exactly the mediant $\frac{a+c}{b+d}$.*

The discovery of this curious phenomenon in the early 1800s was initially attributed to a geologist and amateur mathematician named Farey, although it turned out that he was not the first person to have noticed it. In spite of this confusion, the sequence of fractions a/b between 0 and 1 with denominator less than or equal to a given number n is usually called the nth *Farey series* F_n. For example, here is F_7:

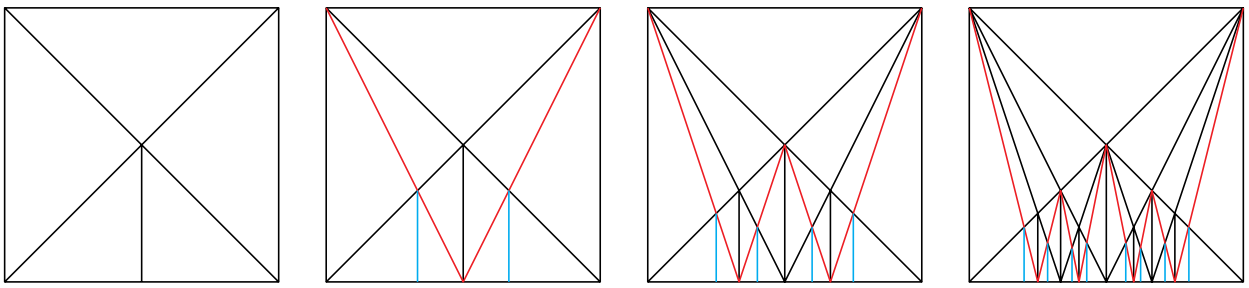
$$\frac{0}{1}\ \frac{1}{7}\ \frac{1}{6}\ \frac{1}{5}\ \frac{1}{4}\ \frac{2}{7}\ \frac{1}{3}\ \frac{2}{5}\ \frac{3}{7}\ \frac{1}{2}\ \frac{4}{7}\ \frac{3}{5}\ \frac{2}{3}\ \frac{5}{7}\ \frac{3}{4}\ \frac{4}{5}\ \frac{5}{6}\ \frac{6}{7}\ \frac{1}{1}$$

These numbers trace out the up-and-down path across the bottom of the figure above. For the next Farey series F_8 we would insert $1/8$ between $0/1$ and $1/7$, $3/8$ between $1/3$ and $2/5$, $5/8$ between $3/5$ and $2/3$, and finally $7/8$ between $6/7$ and $1/1$.

There is a cleaner way to draw the preceding diagram using straight lines in a square:

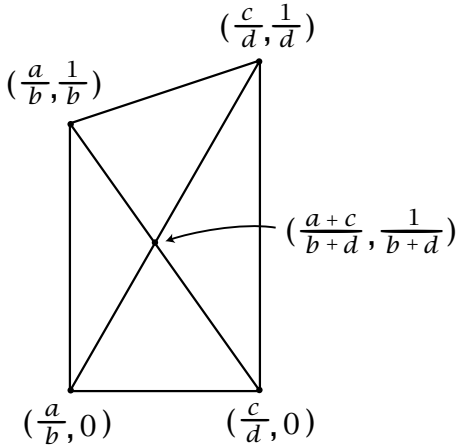


One can construct this diagram in stages, as indicated in the sequence of figures below. Start with a square together with its diagonals and a vertical line from their intersection point down to the bottom edge of the square. Next, connect the resulting midpoint of the lower edge of the square to the two upper corners of the square and drop vertical lines down from the two new intersection points this produces. Now add a W-shaped zigzag and drop verticals again. It should then be clear how to continue.



A nice feature of this construction is that if we start with a square whose sides have length 1 and place this square so that its bottom edge lies along the x-axis with the lower left corner of the square at the origin, then the construction assigns labels to the vertices along the bottom edge of the square that are exactly the x coordinates of these points. Thus the vertex labeled $1/2$ really is at the midpoint of the bottom edge of the square, and the vertices labeled $1/3$ and $2/3$ really are $1/3$ and $2/3$ of the way along this edge, and so forth. In order to verify this fact the key observation is the

following: For a vertical line segment in the diagram whose lower endpoint is at the point $(\frac{a}{b}, 0)$ on the x-axis, the upper endpoint is at the point $(\frac{a}{b}, \frac{1}{b})$. This is obviously true at the first stage of the construction, and it continues to hold at each successive stage since for a quadrilateral whose four vertices have coordinates as shown in the figure at the right, the two diagonals intersect at the point $(\frac{a+c}{b+d}, \frac{1}{b+d})$. For example, to verify that $(\frac{a+c}{b+d}, \frac{1}{b+d})$ is on the line from $(\frac{a}{b}, 0)$ to $(\frac{c}{d}, \frac{1}{d})$ it suffices to show that the line segments from $(\frac{a}{b}, 0)$ to $(\frac{a+c}{b+d}, \frac{1}{b+d})$ and from $(\frac{a+c}{b+d}, \frac{1}{b+d})$ to $(\frac{c}{d}, \frac{1}{d})$ have the same slope. These slopes are



$$\frac{1/(b+d) - 0}{(a+c)/(b+d) - a/b} \cdot \frac{b(b+d)}{b(b+d)} = \frac{b}{b(a+c) - a(b+d)} = \frac{b}{bc - ad}$$

and

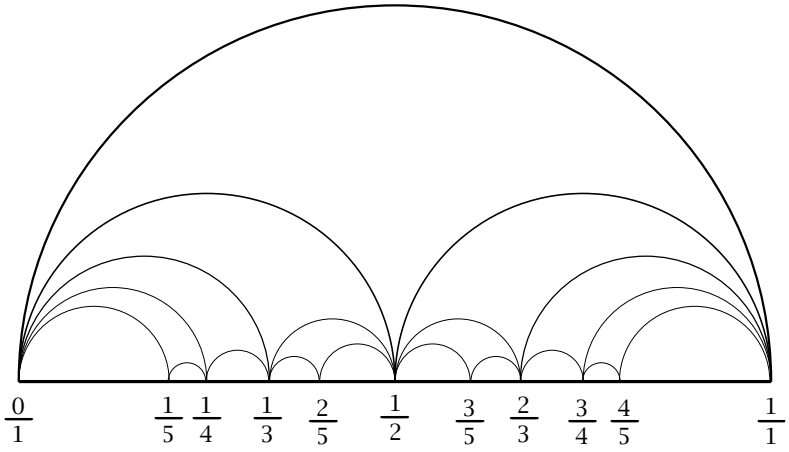
$$\frac{1/d - 1/(b+d)}{c/d - (a+c)/(b+d)} \cdot \frac{d(b+d)}{d(b+d)} = \frac{b+d-d}{c(b+d) - d(a+c)} = \frac{b}{bc - ad}$$

so they are equal. The same argument works for the other diagonal, just by interchanging $\frac{a}{b}$ and $\frac{c}{d}$.

Going back to the square diagram, this fact that we have just shown implies that the successive Farey series can be obtained by taking the vertices that lie above the line $y = \frac{1}{2}$, then the vertices above $y = \frac{1}{3}$, then above $y = \frac{1}{4}$, and so on. Here we are assuming the two properties of the Farey diagram that will be shown in the next chapter, that all rational numbers occur eventually as labels on vertices, and that these labels are always fractions in lowest terms.

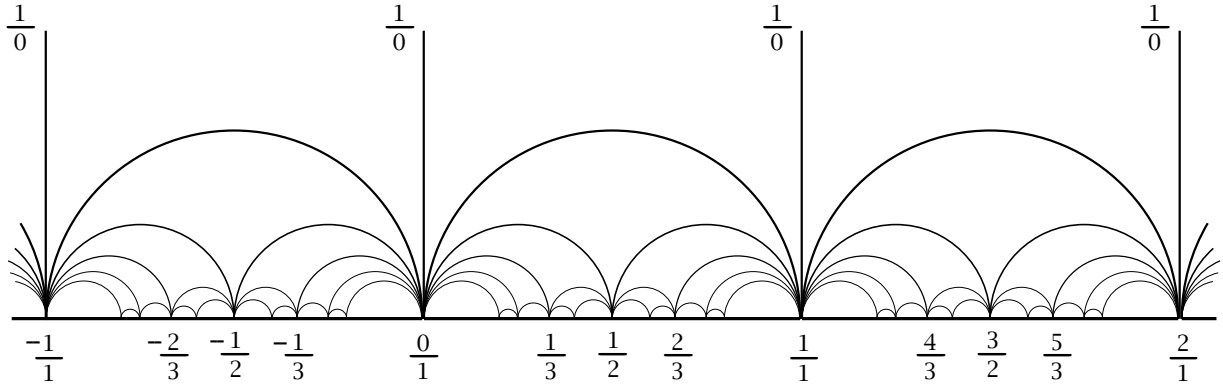
The Upper Half-Plane Farey Diagram

In the square diagram depicting the Farey series, the most important thing for our purposes is the triangles, not the vertical lines. We can get rid of all the vertical lines by shrinking each one to its lower endpoint, converting each triangle into a curvilinear triangle with semicircles as edges, as shown in the diagram below.



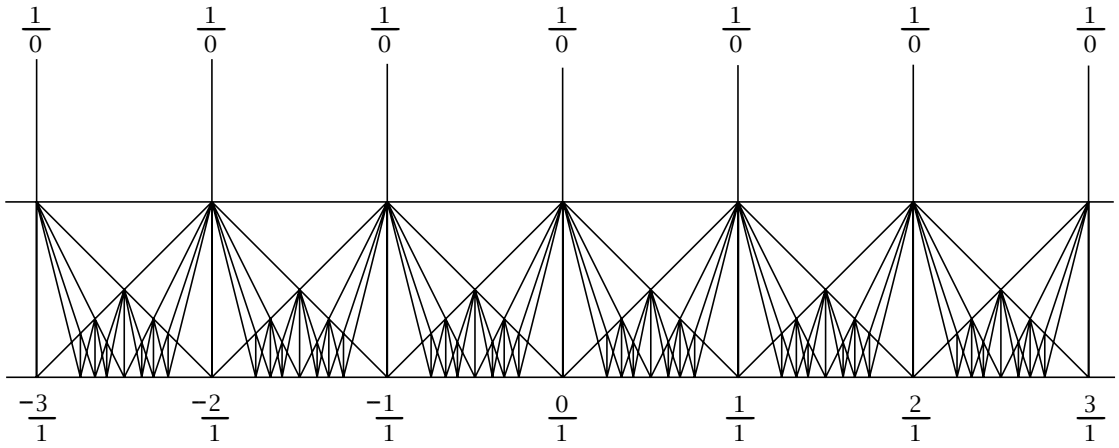
This looks more like a portion of the Farey diagram we started with at the beginning of the chapter, but with the outer boundary circle straightened into a line. The advantage of the new version is that the labels on the vertices are exactly in their correct places along the x-axis, so the vertex labeled $\frac{a}{b}$ is exactly at the point $\frac{a}{b}$ on the x-axis.

This diagram can be enlarged so as to include similar diagrams for fractions between all pairs of adjacent integers, not just 0 and 1, all along the x-axis:



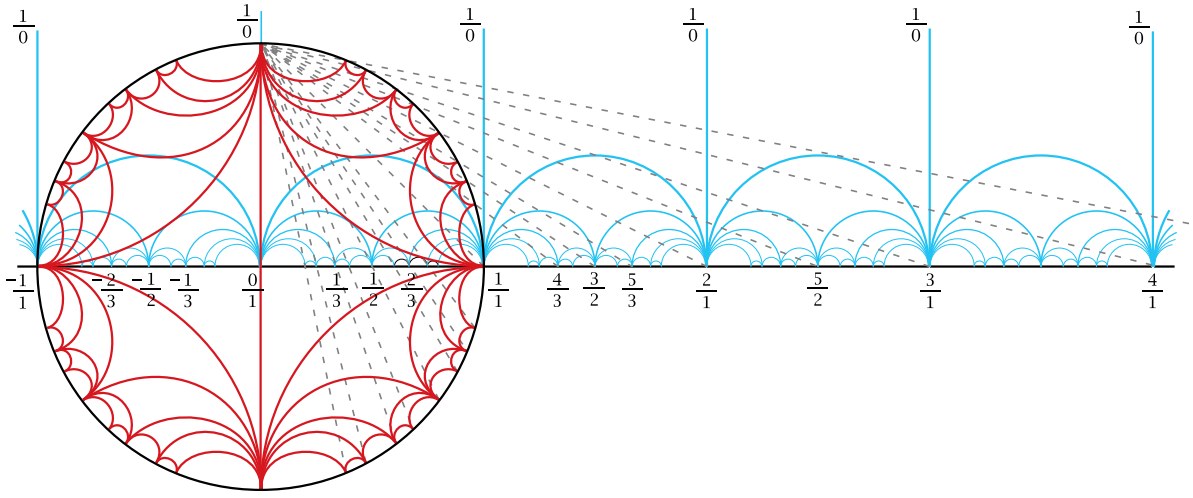
We can also put in vertical lines at the integer points, extending upward to infinity. These correspond to the edges having one endpoint at the vertex $1/0$ in the original Farey diagram.

We could also form a linear version of the full Farey diagram from copies of the square:

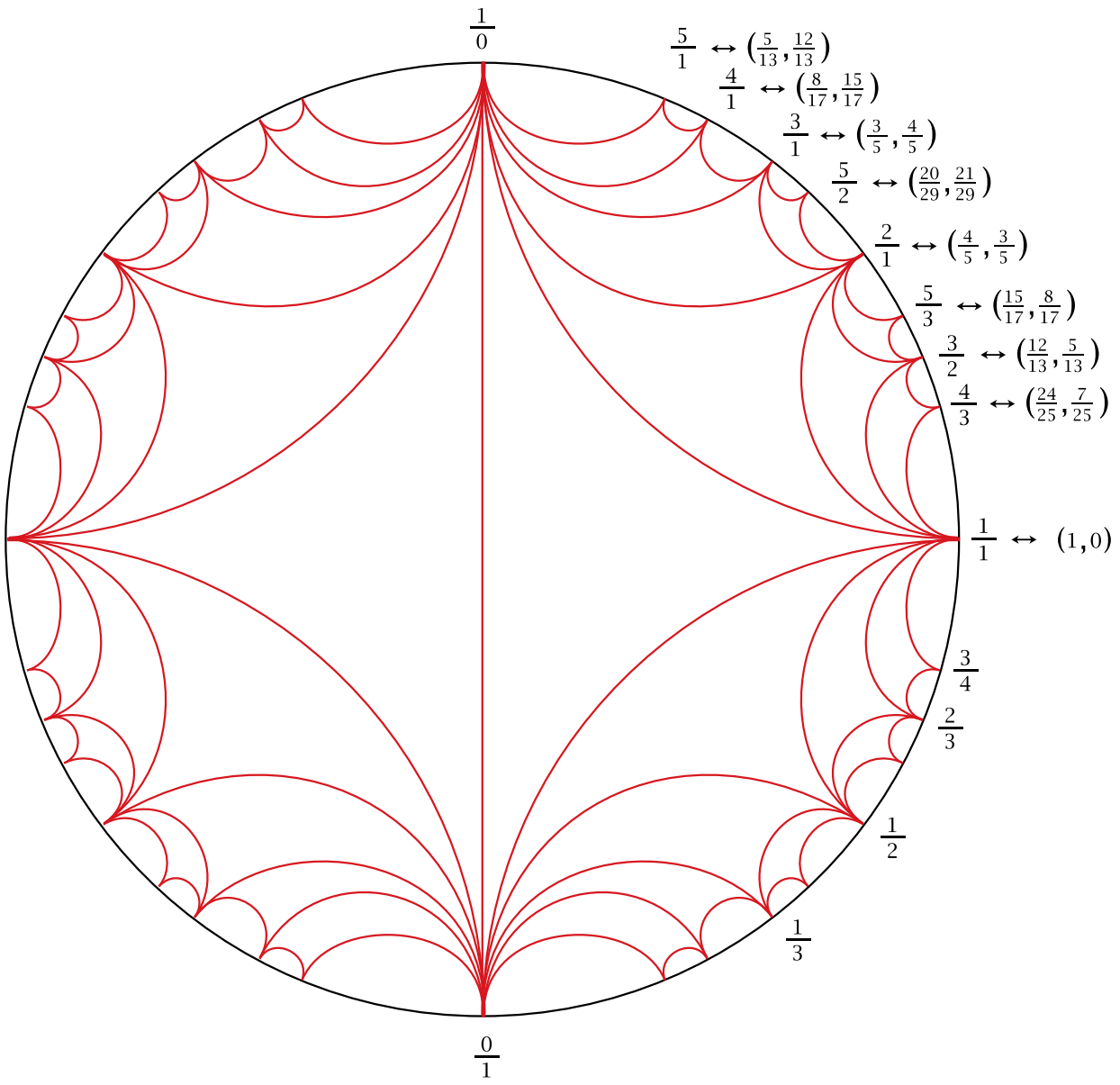


Relation with Pythagorean Triples

Next we describe a variant of the circular Farey diagram that is closely related to Pythagorean triples. Recall from Chapter 0 that rational points (x, y) on the unit circle correspond to rational points p/q on the x-axis by means of lines through the point $(0, 1)$ on the circle. In formulas, $(x, y) = (\frac{2pq}{p^2+q^2}, \frac{p^2-q^2}{p^2+q^2})$. Using this correspondence, we can label the rational points on the circle by the corresponding rational points on the x-axis and then construct a new Farey diagram in the circle by filling in triangles by the mediant rule just as before.



The result is a version of the circular Farey diagram that is rotated by 90 degrees to put $1/0$ at the top of the circle, and there are also some perturbations of the positions of the other vertices and the shapes of the triangles. The next figure shows an enlargement of the new part of the diagram, with the vertices labeled by both the fraction p/q and the coordinates (x, y) of the vertex:



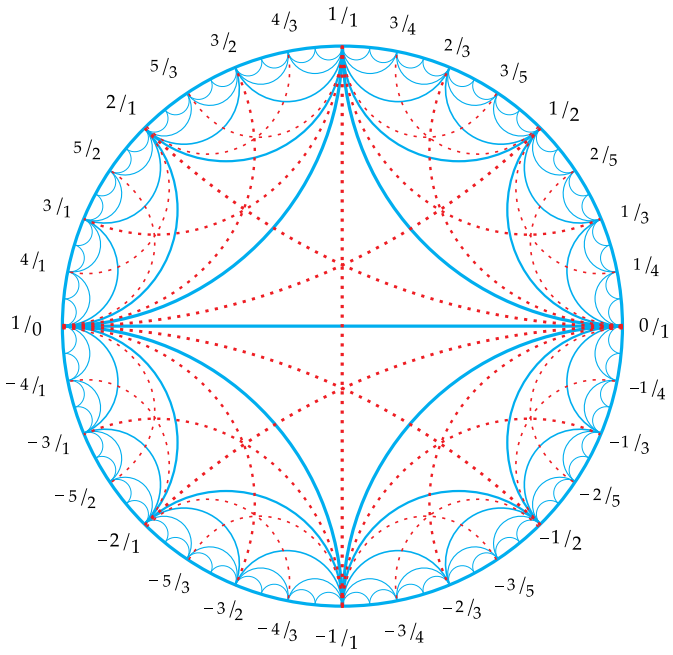
The Determinant Rule for Edges

The construction we have described for the Farey diagram involves an inductive process, where more and more triangles are added in succession. With a construction like this it is not easy to tell by a simple calculation whether or not two given rational numbers a/b and c/d are joined by an edge in the diagram. Fortunately there is such a criterion:

> *Two rational numbers a/b and c/d are joined by an edge in the Farey diagram exactly when the determinant $ad-bc$ of the matrix $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$ is ± 1. This applies also when one of a/b or c/d is $\pm 1/0$.*

We will prove this in the next chapter. What it means in terms of the standard Farey diagram is that if one were to start with the upper half of the xy-plane and insert vertical lines through all the integer points on the x-axis, and then insert semicircles perpendicular to the x-axis joining each pair of rational points a/b and c/d such

that $ad - bc = \pm 1$, then no two of these vertical lines or semicircles would cross, and they would divide the upper half of the plane into non-overlapping triangles. This is really quite remarkable when you think about it, and it does not happen for other values of the determinant besides ± 1. For example, for determinant ± 2 the edges would be the dotted lines in the figure below. Here there are three lines crossing in each triangle of the original Farey diagram, and these lines divide each triangle of the Farey diagram into six smaller triangles.



Exercises

1. This problem involves another version of the Farey diagram, or at least the positive part of the diagram, the part consisting of the triangles whose vertices are labeled by fractions p/q with $p \geq 0$ and $q \geq 0$. In this variant of the diagram the vertex labeled p/q is placed at the point (q, p) in the plane. Thus p/q is the slope of the line through the origin and (q, p). The edges of this new Farey diagram are straight line segments connecting the pairs of vertices that are connected in the original Farey diagram. For example there is a triangle with vertices $(1, 0)$, $(0, 1)$, and $(1, 1)$ corresponding to the big triangle in the upper half of the circular Farey diagram.

What you are asked to do in this problem is just to draw the portion of the new Farey diagram consisting of all the triangles whose vertices (q, p) satisfy $0 \leq q \leq 5$ and $0 \leq p \leq 5$. Note that since fractions p/q labeling vertices are always in lowest terms, the points (q, p) such that q and p have a common divisor greater than 1 are not vertices of the diagram.

A parenthetical comment: With this model of the Farey diagram the operation of forming the mediant of two fractions just corresponds to standard vector addition $(a, b) + (c, d) = (a + c, b + d)$, which may make the mediant operation seem more natural.

2. Compute the Farey series F_{10}.

Chapter 2. Continued Fractions

Here are two typical examples of continued fractions:

$$\frac{7}{16} = \cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{2}}} \qquad \frac{67}{24} = 2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{4}}}}$$

To compute the value of a continued fraction one starts in the lower right corner and works one's way upward. For example in the continued fraction for $\frac{7}{16}$ one starts with $3+\frac{1}{2}=\frac{7}{2}$, then taking 1 over this gives $\frac{2}{7}$, and adding the 2 to this gives $\frac{16}{7}$, and finally 1 over this gives $\frac{7}{16}$.

Here is the general form of a continued fraction:

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1+\cfrac{1}{a_2+\ddots+\cfrac{1}{a_n}}}$$

To write this in more compact form on a single line one can write it as

$$\frac{p}{q} = a_0 + 1\!\!\diagup\!\!a_1 + 1\!\!\diagup\!\!a_2 + \cdots + 1\!\!\diagup\!\!a_n$$

For example:

$$\frac{7}{16} = 1\!\!\diagup\!\!2 + 1\!\!\diagup\!\!3 + 1\!\!\diagup\!\!2 \qquad \frac{67}{24} = 2 + 1\!\!\diagup\!\!1 + 1\!\!\diagup\!\!3 + 1\!\!\diagup\!\!1 + 1\!\!\diagup\!\!4$$

To compute the continued fraction for a given rational number one starts in the upper left corner and works one's way downward, as the following example shows:

$$\frac{67}{24} = 2+\frac{19}{24} = 2+\frac{1}{24/19} = 2+\frac{1}{1+5/19} = 2+\cfrac{1}{1+\cfrac{1}{19/5}}$$

$$= 2+\cfrac{1}{1+\cfrac{1}{3+4/5}} = 2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{5/4}}} = 2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{4}}}}$$

If one is good at mental arithmetic and the numbers aren't too large, only the final form of the answer needs to be written down: $\frac{67}{24} = 2 + 1\!\!\diagup\!\!1 + 1\!\!\diagup\!\!3 + 1\!\!\diagup\!\!1 + 1\!\!\diagup\!\!4$.

The Euclidean Algorithm

The process for computing the continued fraction for a given rational number is known as the *Euclidean Algorithm*. It consists of repeated division, at each stage dividing the previous remainder into the previous divisor. The procedure for $67/24$ is shown at the right. Note that the numbers in the shaded box are the numbers a_i in the continued fraction. These are the quotients of the successive divisions. They are sometimes called the *partial quotients* of the original fraction.

$$\begin{aligned} 67 &= 2\cdot 24 + 19 \\ 24 &= 1\cdot 19 + 5 \\ 19 &= 3\cdot 5 + 4 \\ 5 &= 1\cdot 4 + 1 \\ 4 &= 4\cdot 1 + 0 \end{aligned}$$

One of the classical uses for the Euclidean algorithm is to find the greatest common divisor of two given numbers. If one applies the algorithm to two numbers p and q, dividing the smaller into the larger, then the remainder into the first divisor, and so on, then the greatest common divisor of p and q turns out to be the last nonzero remainder. For example, starting with $p = 72$ and $q = 201$ the calculation is shown at the right, and the last nonzero remainder is 3, which is the greatest common divisor of 72 and 201. (In fact the fraction $201/72$ equals $67/24$, which explains why the successive quotients for this example are the same as in the preceding example.) It is easy to see from the displayed equations why 3 has to be the greatest common divisor of 72 and 201, since from the first equation it follows that any divisor of 72 and 201 must also divide 57, then the second equation shows it must divide 15, the third equation then shows it must divide 12, and the fourth equation shows it must divide 3, the last nonzero remainder. Conversely, if a number divides the last nonzero remainder 3, then the last equation shows it must also divide the 12, and the next-to-last equation then shows it must divide 15, and so on until we conclude that it divides all the numbers not in the shaded rectangle, including the original two numbers 72 and 201. The same reasoning applies in general.

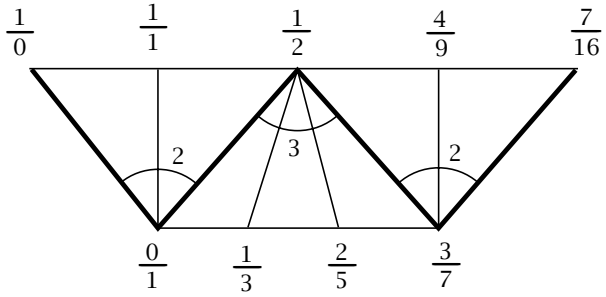
$$\begin{aligned} 201 &= 2\cdot 72 + 57 \\ 72 &= 1\cdot 57 + 15 \\ 57 &= 3\cdot 15 + 12 \\ 15 &= 1\cdot 12 + \textcircled{3} \\ 12 &= 4\cdot 3 + 0 \end{aligned}$$

A more obvious way to try to compute the greatest common divisor of two numbers would be to factor each of them into a product of primes, then look to see which primes occurred as factors of both, and to what power. But to factor a large number into its prime factors is a very laborious and time-consuming process. For example, even a large computer would have a hard time factoring a number of a hundred digits into primes, so it would not be feasible to find the greatest common divisor of a pair of hundred-digit numbers this way. However, the computer would have no trouble at all applying the Euclidean algorithm to find their greatest common divisor.

Having seen what continued fractions are, let us now see what they have to do with the Farey diagram. Some examples will illustrate this best, so let us first look at the continued fraction for $7/16$ again. This has $2, 3, 2$ as its sequence of partial quotients.

We use these three numbers to build a strip of three large triangles subdivided into 2, 3, and 2 smaller triangles, from left to right:

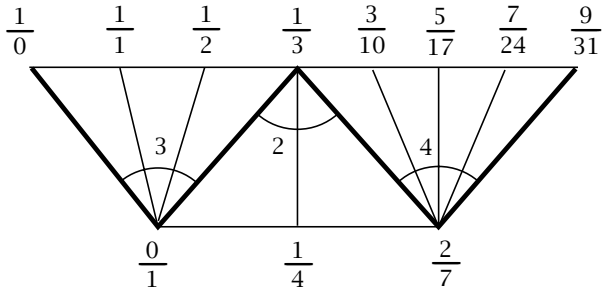
$$\frac{7}{16} = \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{2}}}$$



We can think of the diagram as being formed from three “fans", where the first fan is made from the first 2 small triangles, the second fan from the next 3 small triangles, and the third fan from the last 2 small triangles. Now we begin labeling the vertices of this strip. On the left edge we start with the labels $1/0$ and $0/1$. Then we use the mediant rule for computing the third label of each triangle in succession as we move from left to right in the strip. Thus we insert, in order, the labels $1/1$, $1/2$, $1/3$, $2/5$, $3/7$, $4/9$, and finally $7/16$.

Was it just an accident that the final label was the fraction $7/16$ that we started with, or does this always happen? Doing more examples should help us decide. Here is a second example:

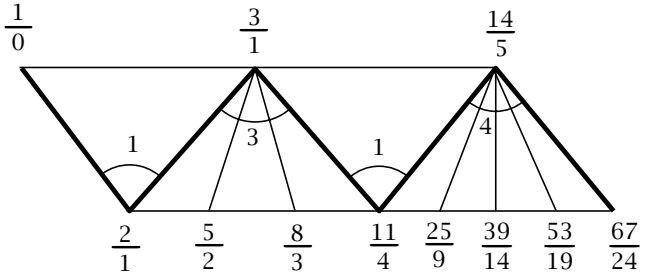
$$\frac{9}{31} = \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{4}}}$$



Again the final vertex on the right has the same label as the fraction we started with. The reader is encouraged to try more examples to make sure we are not rigging things to get a favorable outcome by only choosing examples that work.

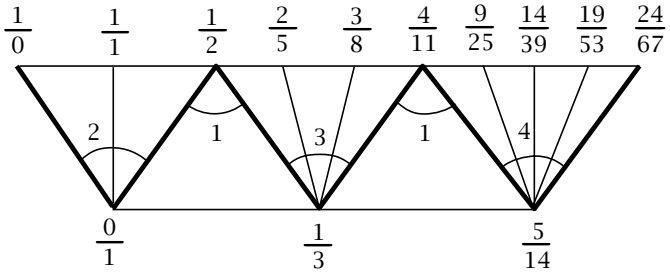
In fact this always works for fractions p/q between 0 and 1. For fractions larger than 1 the procedure works if we modify it by replacing the label $0/1$ with the initial integer $a_0/1$ in the continued fraction $a_0 + {}^{1}\!/_{a_1} + {}^{1}\!/_{a_2} + \cdots + {}^{1}\!/_{a_n}$. This is illustrated by the $67/24$ example:

$$\frac{67}{24} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4}}}}$$



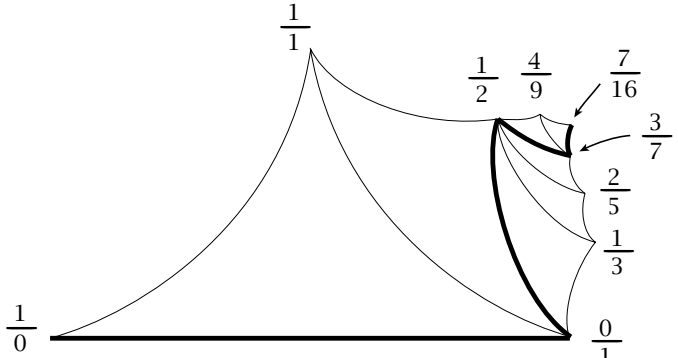
For comparison, here is the corresponding strip for the reciprocal, $24/67$:

$$\frac{24}{67} = \cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{4}}}}}$$



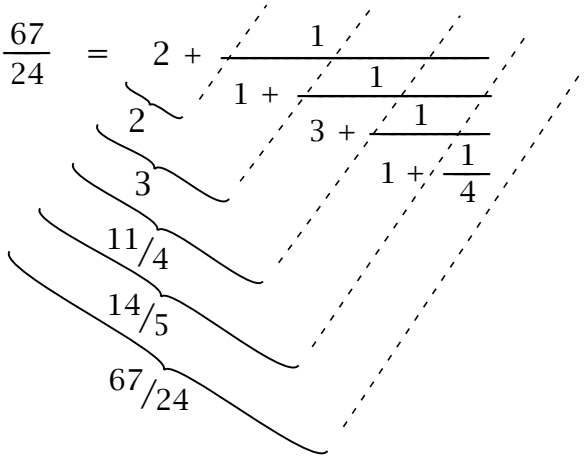
Now let us see how all this relates to the Farey diagram. Since the rule for labeling vertices in the triangles along the horizontal strip for a fraction p/q is the mediant rule, each of the triangles in the strip is a triangle in the Farey diagram, somewhat distorted in shape, and the strip of triangles can be regarded as a sequence of adjacent triangles in the diagram. Here is what this looks like for the fraction $7/16$ in the circular Farey diagram, slightly distorted for the sake of visual clarity:

$$\frac{7}{16} = \cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{2}}}$$



In the strip of triangles for a fraction p/q there is a zigzag path from $1/0$ to p/q that we have indicated by the heavily shaded edges. The vertices that this zigzag path passes through have a special significance. They are the fractions that occur as the values of successively larger initial portions of the continued fraction, as illustrated in the following example:

$$\frac{67}{24} = 2 + \cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{4}}}}$$



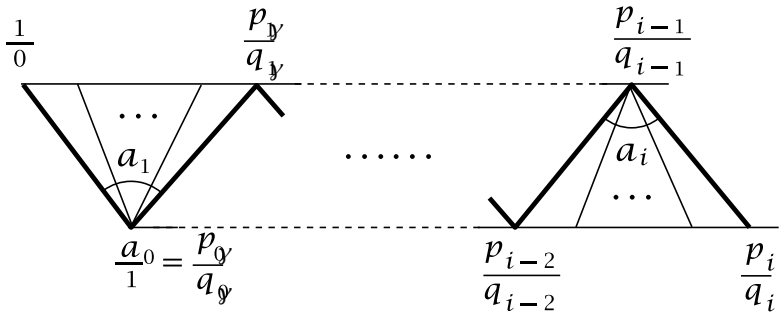
These fractions are called the *convergents* for the given fraction. Thus the convergents for $67/24$ are 2, 3, $11/4$, $14/5$, and $67/24$ itself.

From the preceding examples one can see that each successive vertex label p_i/q_i along the zigzag path for a continued fraction $\frac{p}{q} = a_0 + 1/a_1 + 1/a_2 + \cdots + 1/a_n$ is

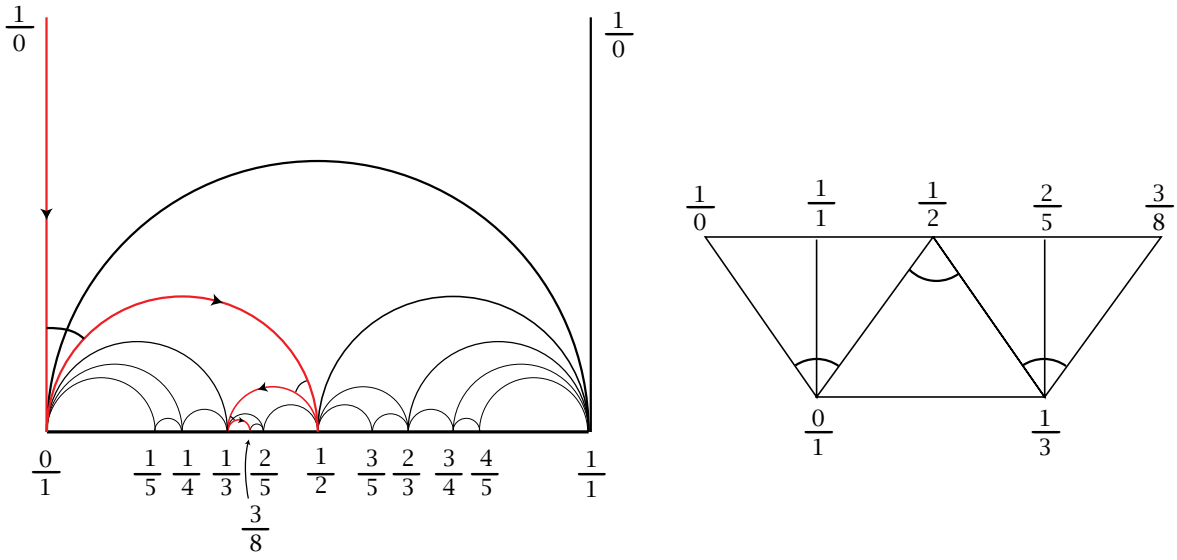
computed in terms of the two preceding vertex labels according to the rule

$$\frac{p_i}{q_i} = \frac{a_i p_{i-1} + p_{i-2}}{a_i q_{i-1} + q_{i-2}}$$

This is because the mediant rule is being applied a_i times, 'adding' p_{i-1}/q_{i-1} to the previously obtained fraction each time until the next label p_i/q_i is obtained.



It is interesting to see what the zigzag paths corresponding to continued fractions look like in the upper half-plane Farey diagram. The next figure shows the simple example of the continued fraction for $3/8$. We can see here that the five triangles of the strip correspond to the four curvilinear triangles lying directly above $3/8$ in the Farey diagram, plus the fifth 'triangle' extending upward to infinity, bounded on the left and right by the vertical lines above $0/1$ and $1/1$, and bounded below by the semicircle from $0/1$ to $1/1$.



This example is typical of the general case, where the zigzag path for a continued fraction $\frac{p}{q} = a_0 + 1/a_1 + 1/a_2 + \cdots + 1/a_n$ becomes a 'pinball path' in the Farey diagam, starting down the vertical line from $1/0$ to $a_0/1$, then turning left across a_1 triangles, then right across a_2 triangles, then left across a_3 triangles, continuing to alternate left and right turns until reaching the final vertex p/q. Two consequences of this are:

(1) The convergents are alternately smaller than and greater than p/q.

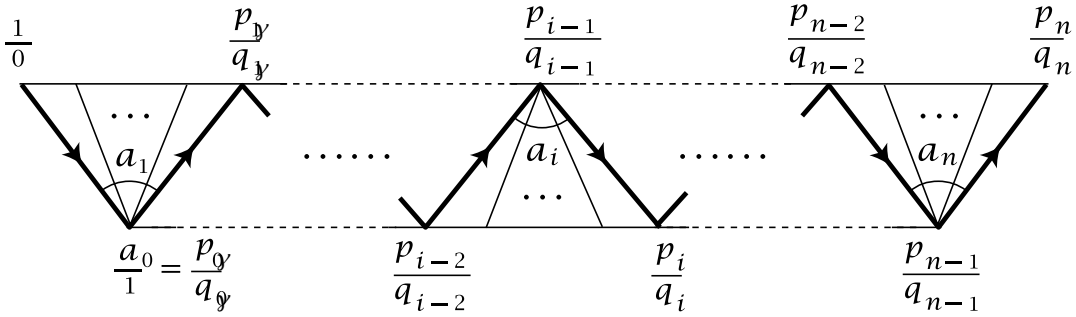
(2) The triangles that form the strip of triangles for p/q are exactly the triangles in the Farey diagram that lie directly above the point p/q on the x-axis.

Here is a general statement describing the relationship between continued fractions and the Farey diagram that we have observed in all our examples so far:

Theorem. *The convergents for the continued fraction* $\frac{p}{q} = a_0 + 1/a_1 + 1/a_2 + \cdots + 1/a_n$ *are the vertices along a zigzag path consisting of a finite sequence of edges in the Farey diagram, starting at* $1/0$ *and ending at* p/q*. The path starts along the edge from* $1/0$ *to* $a_0/1$*, then turns left across a fan of* a_1 *triangles, then right across a fan of* a_2 *triangles, etc., finally ending at* p/q*.*

In particular, since every positive rational number has a continued fraction expansion, we see that every positive rational number occurs eventually as the label of some vertex in the positive half of the diagram. All negative rational numbers then occur as labels in the negative half.

Proof of the Theorem: The continued fraction $\frac{p}{q} = a_0 + 1/a_1 + 1/a_2 + \cdots + 1/a_n$ determines a strip of triangles:



We will show that the label p_n/q_n on the final vertex in this strip is equal to p/q, the value of the continued fraction. Replacing n by i, we conclude that this holds also for each initial seqment $a_0 + 1/a_1 + 1/a_2 + \cdots + 1/a_i$ of the continued fraction. This is just saying that the vertices p_i/q_i along the strip are the convergents to p/q, which is what the theorem claims.

To prove that $p_n/q_n = p/q$ we will use 2×2 matrices. Consider the product

$$P = \begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix}$$

We can multiply this product out starting either from the left or from the right. Suppose first that we multiply starting at the left. The initial matrix is $\begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix}$ and we can view the two columns of this matrix as the two fractions $1/0$ and $a_0/1$ labeling the left edge of the strip of triangles. When we multiply this matrix by the next matrix we get

$$\begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} = \begin{pmatrix} a_0 & 1 + a_0a_1 \\ 1 & a_1 \end{pmatrix} = \begin{pmatrix} p_0 & p_1 \\ q_0 & q_1 \end{pmatrix}$$

The two columns here give the fractions at the ends of the second edge of the zigzag path. The same thing happens for subsequent matrix multiplications, as multiplying by the next matrix in the product takes the matrix corresponding to one edge of the

zigzag path to the matrix corresponding to the next edge:

$$\begin{pmatrix} p_{i-2} & p_{i-1} \\ q_{i-2} & q_{i-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_i \end{pmatrix} = \begin{pmatrix} p_{i-1} & p_{i-2} + a_i p_{i-1} \\ q_{i-1} & q_{i-2} + a_i q_{i-1} \end{pmatrix} = \begin{pmatrix} p_{i-1} & p_i \\ q_{i-1} & q_i \end{pmatrix}$$

In the end, when all the matrices have been multiplied, we obtain the matrix corresponding to the last edge in the strip from p_{n-1}/q_{n-1} to p_n/q_n. Thus the second column of the product P is p_n/q_n, and what remains is to show that this equals the value p/q of the continued fraction $a_0 + 1/(a_1 + 1/(a_2 + \cdots + 1/a_n))$.

The value of the continued fraction $a_0 + 1/(a_1 + 1/(a_2 + \cdots + 1/a_n))$ is computed by working from right to left. If we let r_i/s_i be the value of the tail $1/(a_i + 1/(a_{i+1} + \cdots + 1/a_n))$ of the continued fraction, then $r_n/s_n = 1/a_n$ and we have

$$\frac{r_i}{s_i} = \frac{1}{a_i + \dfrac{r_{i+1}}{s_{i+1}}} = \frac{s_{i+1}}{a_i s_{i+1} + r_{i+1}} \qquad \text{and finally} \qquad \frac{p}{q} = a_0 + \frac{r_1}{s_1} = \frac{a_0 s_1 + r_1}{s_1}$$

In terms of matrices this implies that we have

$$\begin{pmatrix} r_n \\ s_n \end{pmatrix} = \begin{pmatrix} 1 \\ a_n \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & a_i \end{pmatrix} \begin{pmatrix} r_{i+1} \\ s_{i+1} \end{pmatrix} = \begin{pmatrix} s_{i+1} \\ r_{i+1} + a_i s_{i+1} \end{pmatrix} = \begin{pmatrix} r_i \\ s_i \end{pmatrix}$$

$$\text{and} \quad \begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r_1 \\ s_1 \end{pmatrix} = \begin{pmatrix} r_1 + a_0 s_1 \\ s_1 \end{pmatrix} = \begin{pmatrix} p \\ q \end{pmatrix}$$

This means that when we multiply out the product P starting from the right, then the second columns will be successively $\begin{pmatrix} r_n \\ s_n \end{pmatrix}$, $\begin{pmatrix} r_{n-1} \\ s_{n-1} \end{pmatrix}$, $\cdots$, $\begin{pmatrix} r_1 \\ s_1 \end{pmatrix}$ and finally $\begin{pmatrix} p \\ q \end{pmatrix}$. We already showed this second column is $\begin{pmatrix} p_n \\ q_n \end{pmatrix}$, so $p/q = p_n/q_n$ and the proof is complete. □

An interesting fact that can be deduced from the preceding proof is that for a continued fraction $1/(a_1 + 1/(a_2 + \cdots + 1/a_n))$ with no initial integer a_0, if we reverse the order of the numbers a_i, this leaves the denominator unchanged. For example

$$1/(2 + 1/(3 + 1/4)) = \frac{13}{30} \qquad \text{and} \qquad 1/(4 + 1/(3 + 1/2)) = \frac{7}{30}$$

To see why this must always be true we use the operation of transposing a matrix to interchange its rows and columns. For a 2×2 matrix this just amounts to interchanging the upper-right and lower-left entries:

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}^T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Transposing a product of matrices reverses the order of the factors: $(AB)^T = B^T A^T$, as can be checked by direct calculation. In the product

$$\begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix}$$

the individual matrices on the left side of the equation are symmetric with respect to transposition, so the transpose of the product is obtained by just reversing the order of the factors:

$$\begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_{n-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} = \begin{pmatrix} p_{n-1} & q_{n-1} \\ p_n & q_n \end{pmatrix}$$

Thus the denominator q_n is unchanged, as claimed.

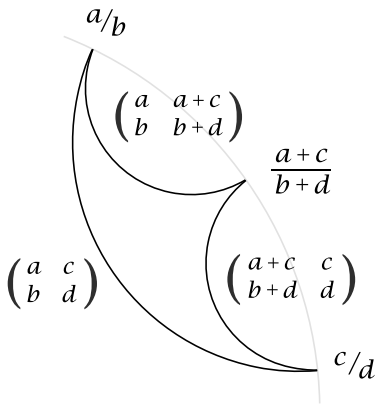
There is also a fairly simple relationship between the numerators. In the example of $13/30$ and $7/30$ we see that the product of the numerators, 91, is congruent to 1 modulo the denominator. In the general case the product of the numerators is $p_n q_{n-1}$ and this is congruent to $(-1)^{n+1}$ modulo the denominator q_n. To verify this, we note that the determinant of each factor $\begin{pmatrix} 0 & 1 \\ 1 & a_i \end{pmatrix}$ is -1 so since the determinant of a product is the product of the determinants, we have $p_{n-1}q_n - p_n q_{n-1} = (-1)^n$, which says that $p_n q_{n-1}$ is congruent to $(-1)^{n+1}$ modulo q_n.

Determinants Determine Edges

We constructed the Farey diagram by an inductive procedure, inserting successive edges according to the mediant rule, but there is another rule that can be used to characterize the edges in the diagram:

Theorem. *In the Farey diagram, two vertices labeled a/b and c/d are joined by an edge if and only if the determinant $ad - bc$ of the matrix $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$ is equal to ± 1.*

Proof: First we show that for an arbitrary edge in the diagram joining a/b to c/d, the associated matrix $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$ has determinant ± 1. This is obviously true for the edges in the two largest triangles in the circular version of the diagram. For the smaller triangles we proceed by induction. The figure at the right shows the three matrices corresponding to the edges of one of these smaller triangles. By induction we assume we know that $ad - bc = \pm 1$ for the long edge of the triangle. Then the determinant condition holds also for the two shorter edges of the triangle since $a(b+d) - b(a+c) = ad - bc$ and $(a+c)d - (b+d)c = ad - bc$.



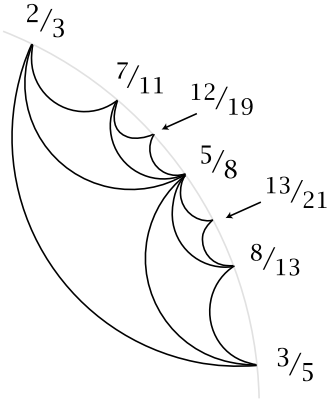
Before proving the converse let us pause to apply what we have shown so far to deduce a basic fact about the Farey diagram that was mentioned but not proved when we first constructed the diagram:

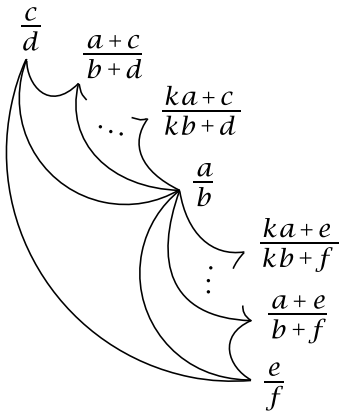
Corollary. *The mediant rule for labeling the vertices in the Farey diagram always produces labels a/b that are fractions in lowest terms.*

Proof: Consider an edge joining a vertex labeled a/b to some other vertex labeled c/d. By the preceding proposition we know that $ad - bc = \pm 1$. This equation implies

that a and b can have no common divisor greater than 1 since any common divisor of a and b must divide the products ad and bc, hence also the difference $ad-bc = \pm 1$, but the only divisors of ± 1 are ± 1. □

Now we return to proving the converse half of the theorem, which says that there is an edge joining a/b to c/d whenever $ad-bc = \pm 1$. To do this we will examine how all the edges emanating from a fixed vertex a/b are related. To begin, if $a/b = 0/1$ then the matrices $\begin{pmatrix} 0 & c \\ 1 & d \end{pmatrix}$ with determinant ± 1 are the matrices $\begin{pmatrix} 0 & \pm 1 \\ 1 & d \end{pmatrix}$, and these correspond exactly to the edges in the diagram from $0/1$ to $\pm 1/d$. There is a similar exact correspondence for the edges from $1/0$. For the other vertices a/b, the example $a/b = 5/8$ is shown in the left half of the figure below. The first edges drawn to this vertex come from $2/3$ and $3/5$, and after this all the other edges from $5/8$ are drawn in turn. As one can see, they are all obtained by adding $(5,8)$ to $(2,3)$ or $(3,5)$ repeatedly. If we choose any one of these edges from $5/8$, say the edge to $2/3$ for example, then the edges from $5/8$ have their other endpoints at the fractions $(2+5k)/(3+8k)$ as k ranges over all integers, with positive values of k giving the edges on the upper side of the edge to $2/3$ and negative values of k giving the edges on the lower side of the edge to $2/3$.





The same thing happens for an arbitrary value of a/b as shown in the right half of the figure, where a/b initially arises as the mediant of c/d and e/f. In this case if we choose the edge to c/d as the starting edge, then the other edges go from a/b to $(c+ka)/(d+kb)$. In particular, when $k = -1$ we get the edge to $(c-a)/(d-b) = (a-c)/(b-d) = e/f$.

To finish the argument we need to know how the various matrices $\left(\begin{smallmatrix} a & x \\ b & y \end{smallmatrix}\right)$ of determinant $ay - bx = \pm 1$ having the same first column are related. This can be deduced from the following result about integer solutions of linear equations with integer coefficients:

Lemma. *Suppose a and b are integers with no common divisor. If one solution of $ay - bx = n$ is $(x,y) = (c,d)$, then the general solution is $(x,y) = (c+ka, d+kb)$ for k an arbitrary integer.*

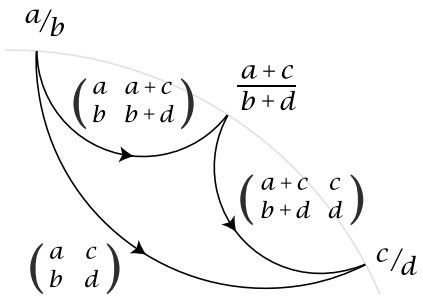
The proof will use the same basic argument as is used in linear algebra to show that the general solution of a system of nonhomogeneous linear equations is obtained from any particular solution by adding the general solution of the associated system of homogeneous equations.

Proof: One solution $(x,y) = (c,d)$ of $ay - bx = n$ is given. For an arbitrary solution (x,y) we look at the difference $(x_0,y_0) = (x-c, y-d)$. This satisfies $ay_0 - bx_0 = 0$, or in other words, $ay_0 = bx_0$. Since a and b have no common divisors, the equation $ay_0 = bx_0$ implies that x_0 must be a multiple of a and y_0 must be a multiple of b, in fact the same multiple in both cases so that the equation becomes $a(kb) = b(ka)$. Thus we have $(x_0,y_0) = (ka,kb)$ for some integer k. Thus every solution of $ay - bx = n$ has the form $(x,y) = (c + x_0, d + y_0) = (c + ka, d + kb)$, and it is clear that these formulas for x and y give solutions for all values of k. □

Now we can easily finish the proof of the theorem. The lemma in the cases $n = \pm 1$ implies that the edges in the Farey diagram with a/b at one endpoint account for all matrices $\left(\begin{smallmatrix} a & x \\ b & y \end{smallmatrix}\right)$ of determinant $ay - bx = \pm 1$. □

There is some ambiguity in the correspondence between edges of the Farey diagram and matrices $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$ of determinant ± 1. For one thing, either column of the matrix can be multiplied by -1, changing the sign of the determinant without changing the value of the fractions a/b and c/d. This ambiguity can be eliminated by choosing all of a, b, c, and d to be positive for edges in the upper half of the circular Farey diagram, and choosing just the numerators a and c to be negative for edges in the lower half of the diagram. The only other ambiguity is that both $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} c & a \\ d & b \end{smallmatrix}\right)$ correspond to the same edge. This ambiguity can be eliminated by orienting the edges by placing an arrowhead on each edge pointing from the vertex corresponding to the first column of the matrix to the vertex corresponding to the second column. Changing the orientation of an edge switches the two columns of the matrix, which changes the sign of the determinant.

The identity matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ has determinant $+1$ and corresponds to the edge from $1/0$ to $0/1$ oriented from left to right in the circular diagram. We can use this orientation to give orientations to all other edges when we build the diagram using the mediant rule. In the upper half of the diagram this makes all edges be oriented toward the right, or in other words from a/b to c/d with $a/b > c/d$. With this orientation, all the corresponding matrices have determinant $+1$ since $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ has determinant $+1$ and we have seen that the determinant doesn't change when we add new edges by the mediant rule. When we use the mediant rule to construct the lower half of the diagram we have to start



with $-1/0$ instead of $1/0$. This means that we are starting with the matrix $\left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)$ instead of $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$. Since the determinant of $\left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)$ is -1, this means that the edges in the lower half of the diagram, when oriented toward the right as in the upper half, correspond to matrices of determinant -1.

The Diophantine Equation ax+by=n

The Euclidean algorithm and continued fractions can be used to compute all the integer solutions of a linear equation $ax + by = n$ where a, b, and n are given integers. We can assume neither a nor b is zero, otherwise the equation is rather trivial. Changing the signs of x or y if necessary, we can rewrite the equation in the form $ax - by = n$ where a and b are both positive.

If a and b have greatest common divisor $d > 1$, then since d divides a and b it must divide $ax - by$, so d must divide n if the equation is to have any solutions at all. If d does divide n we can divide both sides of the equation by d to get a new equation of the same type as the original one and having the same solutions, but with the new coefficients a and b having no common divisors. For example, the equation $6x - 15y = 21$ reduces in this way to the equation $2x - 5y = 7$. Thus we can assume from now on that a and b have no common divisors.

The Lemma from a page or two back shows how to find the general solution of $ax - by = n$ once we have found one particular solution. To find a particular solution it suffices to do the case $n = 1$ since if we have a solution of $ax - by = 1$, we can multiply x and y by n to get a solution of $ax - by = n$. For small values of a and b a solution of $ax - by = 1$ can be found more or less by inspection since the equation $ax - by = 1$ says that we have multiples of a and b that differ by 1. For example, for the equation $2x - 5y = 1$ the smallest multiples of 2 and 5 that differ by 1 are $2 \cdot 3$ and $5 \cdot 1$, so a solution of $2x - 5y = 1$ is $(x, y) = (3, 1)$. A solution of $2x - 5y = 7$ is then $(x, y) = (21, 7)$. By the earlier Lemma, the general solution of $2x - 5y = 7$ is $(x, y) = (21 + 5k, 7 + 2k)$ for arbitrary integers k. The smallest positive solution is $(6, 1)$, obtained by setting $k = -3$. This means we could also write the general solution as $(6 + 5k, 1 + 2k)$.

Solutions of $ax - by = 1$ always exist when a and b have no common divisors, and a way to find one is to find an edge in the Farey diagram with a/b at one end of the edge. This can be done by using the Euclidean algorithm to compute the strip of triangles from $1/0$ to a/b. As an example, let us solve $67x - 24y = 1$. We already computed the strip of triangles for $67/24$ earlier in this chapter. The vertex preceding $67/24$ in the zigzag path is $14/5$ and this vertex lies above $67/24$ so we have $14/5 > 67/24$ and hence the matrix $\left(\begin{smallmatrix}14&67\\5&24\end{smallmatrix}\right)$ has determinant $+1$. Thus one solution of $67x - 24y = 1$ is $(x, y) = (-5, -14)$ and the general solution is $(x, y) = (-5 + 24k, -14 + 67k)$. We could also use the edge from $53/19$ to $67/24$, so $\left(\begin{smallmatrix}67&53\\24&19\end{smallmatrix}\right)$ has determinant $+1$, yielding another formula for the general solution $(19+24k, 53+$

$67k)$.

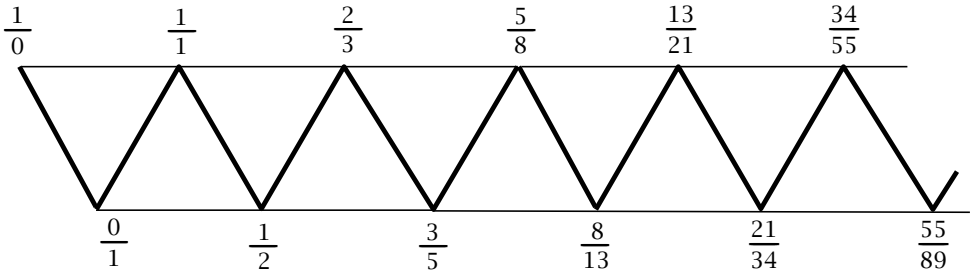
From a geometric point of view, finding the integer solutions of $ax + by = n$ is finding the points on the line $ax + by = n$ in the xy-plane having both coordinates integers. The points in the plane having both coordinates integers form a square grid called the *integer lattice.* Thus we wish to see which points in the integer lattice lie on the line $ax + by = n$. This equation can be written in the form $y = mx + b$ where the slope m and the y-intercept b are both rational. Conversely, an equation $y = mx + b$ with m and b rational can be written as an equation $ax + by = n$ with a, b, and n integers by multiplying through by a common denominator of m and b. Sometimes the equation $ax + by = n$ has no integer solutions, as we have seen, namely when n is not a multiple of the greatest common divisor of a and b, for example the equation $2x+2y = 1$. In these cases the line $ax+by = n$ passes through no integer lattice points. In the opposite case that there does exist an integer solution, there are infinitely many, and they correspond to integer lattice points spaced at equal intervals along the line.

Infinite Continued Fractions

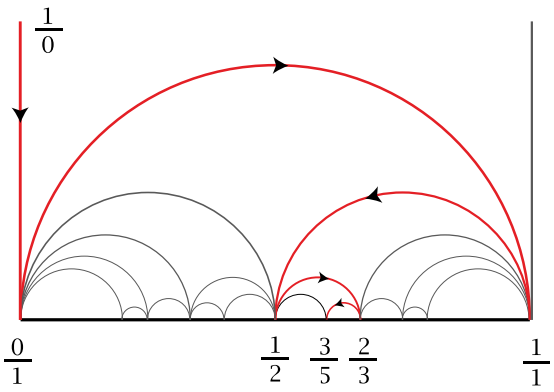
We have seen that all rational numbers can be represented as continued fractions $a_0 + 1/a_1 + 1/a_2 + \cdots + 1/a_n$, but what about irrational numbers? It turns out that these can be represented as *infinite* continued fractions $a_0 + 1/a_1 + 1/a_2 + 1/a_3 + \cdots$. A simple example is $1/1 + 1/1 + 1/1 + \cdots$, or in its expanded form:

$$\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\ddots}}}}$$

The corresponding strip of triangles is infinite:



Notice that these fractions after $1/0$ are the successive ratios of the famous Fibonacci sequence $0, 1, 1, 2, 3, 5, 8, 13, 21, \cdots$ where each number is the sum of its two predecessors. The sequence of convergents is thus $0/1, 1/1, 1/2, 2/3, 3/5, 5/8, 8/13, \cdots$, the vertices along the zigzag path. The way this zigzag path looks in the standard Farey diagram is shown in the figure at the right. What happens when we follow this path farther and farther? The path consists of an infinite sequence of semicircles, each one shorter than the preceding one and sharing a common endpoint. The left endpoints of the semicircles form an increasing sequence of numbers which have to be approaching a certain limiting value x. We know x has to be finite since it is certainly less than each of the right-hand endpoints of the semicircles, the convergents $1/1, 2/3, 5/8, \cdots$. Similarly the right endpoints of the semicircles form a decreasing sequence of numbers approaching a limiting value y greater than each of the left-hand endpoints $0/1, 1/2, 3/5, \cdots$. Obviously $x \le y$. Is it possible that x is not equal to y? If this happened, the infinite sequence of semicircles would be approaching the semicircle from x to y. Above this semicircle there would then be an infinite number of semicircles, all the semicircles in the infinite sequence. Between x and y there would have to be a rational numbers p/q (between any two real numbers there is always a rational number), so above this rational number there would be an infinite number of semicircles, hence an infinite number of triangles in the Farey diagram. But we know that there are only finitely many triangles above any rational number p/q, namely the triangles that appear in the strip for the continued fraction for p/q. This contradiction shows that x has to be equal to y. Thus the sequence of convergents along the edges of the infinite strip of triangles converges to a unique real number x. (This is why the convergents are called convergents.)



This argument works for arbitrary infinite continued fractions, so we have shown the following general result:

Proposition. *For every infinite continued fraction* $a_0 + 1/a_1 + 1/a_2 + 1/a_3 + \cdots$ *the convergents converge to a unique limit.*

This limit is by definition the value of the infinite continued fraction. There is a simple method for computing the value in the example involving Fibonacci numbers. We begin by setting

$$x = 1/1 + 1/1 + 1/1 + \cdots$$

Then if we take the reciprocals of both sides of this equation we get

$$\frac{1}{x} = 1 + 1/1 + 1/1 + 1/1 + \cdots$$

The right side of this equation is just $1+x$, so we can easily solve for x:

$$\begin{aligned}\frac{1}{x} &= 1+x\\ 1 &= x+x^2\\ x^2+x-1 &= 0\\ x &= \frac{-1\pm\sqrt{5}}{2}\end{aligned}$$

We know x is positive, so this rules out the negative root and we are left with the final value $x=(-1+\sqrt{5})/2$. This number, approximately .618, goes by the name of the golden ratio. It has many interesting properties.

Proposition. *Every irrational number has an expression as an infinite continued fraction, and this continued fraction is unique.*

Proof: In the Farey diagram consider the vertical line L going upward from a given irrational number x on the x-axis. The lower endpoint of L is not a vertex of the Farey diagram since x is irrational. Thus as we move downward along L we cross a sequence of triangles, entering each triangle by crossing its upper edge and exiting the triangle by crossing one of its two lower edges. When we exit one triangle we are entering another, the one just below it, so the sequence of triangles and edges we cross must be infinite. The left and right endpoints of the edges in the sequence must be approaching the single point x by the argument we gave in the preceding proposition, so the edges themselves are approaching x. Thus the triangles in the sequence form a single infinite strip consisting of an infinite sequence of fans with their pivot vertices on alternate sides of the strip. The zigzag path along this strip gives a continued fraction for x.

For the uniqueness, we have seen that an infinite continued fraction for x corresponds to a zigzag path in the infinite strip of triangles lying above x. This set of triangles is unique so the strip is unique, and there is only one path in this strip that starts at $1/0$ and then does left and right turns alternately, starting with a left turn. The initial turn must be to the left because the first two convergents are a_0 and $a_0+\frac{1}{a_1}$, with $a_0+\frac{1}{a_1}>a_0$ since $a_1>0$. After the path traverses the first edge, no subsequent edge of the path can go along the border of the strip since this would entail two successive left turns or two successive right turns. □

The arguments we have just given can be used to prove a fact about the standard Farey diagram that we have been taking more or less for granted. This is the fact that the triangles in the diagram completely cover the upper halfplane. In other words, every point (x,y) with $y>0$ lies either in the interior of some triangle or on the common edge between two triangles. To see why, consider the vertical line L in the upper halfplane through the given point (x,y). If x is an integer then (x,y) is on one of the vertical edges of the diagram. Thus we can assume x is not an integer

and hence L is not one of the vertical edges of the diagram. The line L will then be contained in the strip of triangles corresponding to the continued fraction for x. This is a finite strip if x is rational and an infinite strip if x is irrational. In either case the point (x, y), being in L, will be in one of the triangles of the strip or on an edge separating two triangles in the strip. This proves what we wanted to prove.

To compute the infinite continued fraction $a_0 + 1/a_1 + 1/a_2 + 1/a_3 + \cdots$ for a given irrational number x we can follow the same procedure as for rational numbers, but it doesn't terminate after a finite number of steps. Recall the original example that we did:

$$\frac{67}{24} = 2 + \frac{19}{24} = 2 + \frac{1}{24/19} = 2 + \frac{1}{1 + 5/19} = 2 + \frac{1}{1 + \dfrac{1}{19/5}}$$

$$= 2 + \frac{1}{1 + \dfrac{1}{3 + 4/5}} = 2 + \frac{1}{1 + \dfrac{1}{3 + \dfrac{1}{5/4}}} = 2 + \frac{1}{1 + \dfrac{1}{3 + \dfrac{1}{1 + \dfrac{1}{4}}}}$$

The sequence of steps is the following:

(1) Write $x = a_0 + r_1$ where a_0 is an integer and $0 \le r_1 < 1$
(2) Write $1/r_1 = a_1 + r_2$ where a_1 is an integer and $0 \le r_2 < 1$
(3) Write $1/r_2 = a_2 + r_3$ where a_2 is an integer and $0 \le r_3 < 1$

and so on, repeatedly. Thus one first finds the largest integer $a_0 \le x$, with r_1 the 'remainder', then one inverts r_1 and finds the greatest integer $a_1 \le 1/r_1$, with r_2 the remainder, etc.

Here is how this works for $x = \sqrt{2}$:

(1) $\sqrt{2} = 1 + (\sqrt{2} - 1)$ where $a_0 = 1$ since $\sqrt{2}$ is between 1 and 2. Before going on to step (2) we have to compute $\frac{1}{r_1} = \frac{1}{\sqrt{2}-1}$. Multiplying numerator and denominator by $\sqrt{2} + 1$ gives $\frac{1}{\sqrt{2}-1} = \frac{1}{\sqrt{2}-1} \cdot \frac{\sqrt{2}+1}{\sqrt{2}+1} = \sqrt{2} + 1$. This is the number we use in the next step.

(2) $\sqrt{2} + 1 = 2 + (\sqrt{2} - 1)$ since $\sqrt{2} + 1$ is between 2 and 3.

Notice that something unexpected has happened: The remainder $r_2 = \sqrt{2} - 1$ is exactly the same as the previous remainder r_1. There is then no need to do the calculation of $\frac{1}{r_2} = \frac{1}{\sqrt{2}-1}$ since we know it will have to be $\sqrt{2} + 1$. This means that the next step (3) will be exactly the same as step (2), and the same will be true for all subsequent steps. Hence we get the continued fraction

$$\sqrt{2} = 1 + 1/2 + 1/2 + 1/2 + \cdots$$

We can check this calculation by finding the value of the continued fraction in the same way that we did earlier for $1/1 + 1/1 + 1/1 + \cdots$. First we set $x = 1/2 + 1/2 + 1/2 + \cdots$.

Taking reciprocals gives $1/x = 2 + 1/2 + 1/2 + 1/2 + \cdots = 2 + x$. This leads to the quadratic equation $x^2 + 2x - 1 = 0$, which has roots $x = -1 \pm \sqrt{2}$. Since x is positive we can discard the negative root. Thus we have $-1 + \sqrt{2} = 1/2 + 1/2 + 1/2 + \cdots$. Adding 1 to both sides of this equation gives the formula for $\sqrt{2}$ as a continued fraction.

We can get good rational approximations to $\sqrt{2}$ by computing the convergents in its continued fraction $1 + 1/2 + 1/2 + 1/2 + \cdots$. It's a little easier to compute the convergents in $2 + 1/2 + 1/2 + 1/2 + \cdots = 1 + \sqrt{2}$ and then subtract 1 from each of these. For $2 + 1/2 + 1/2 + 1/2 + \cdots$ there is a nice pattern to the convergents:

$$\frac{2}{1}, \frac{5}{2}, \frac{12}{5}, \frac{29}{12}, \frac{70}{29}, \frac{169}{70}, \frac{408}{169}, \frac{985}{408}, \cdots$$

Notice that the sequence of numbers $1, 2, 5, 12, 29, 70, 169, \cdots$ is constructed in a way somewhat analogous to the Fibonacci sequence, except that each number is *twice* the preceding number plus the number before that. (It's easy to see why this has to be true, because each convergent is constructed from the previous one by inverting the fraction and adding 2.) After subtracting 1 from each of these fractions we get the convergents to $\sqrt{2}$:

$$\begin{aligned}
\sqrt{2} &= 1.41421356\cdots \\
1/1 &= 1.00000000\cdots \\
3/2 &= 1.50000000\cdots \\
7/5 &= 1.40000000\cdots \\
17/12 &= 1.41666666\cdots \\
41/29 &= 1.41379310\cdots \\
99/70 &= 1.41428571\cdots \\
239/169 &= 1.41420118\cdots \\
577/408 &= 1.41421568\cdots
\end{aligned}$$

We can compute the continued fraction for $\sqrt{3}$ by the same method as for $\sqrt{2}$, but something slightly different happens:

(1) $\sqrt{3} = 1 + (\sqrt{3} - 1)$ since $\sqrt{3}$ is between 1 and 2. Computing $\frac{1}{\sqrt{3}-1}$, we have $\frac{1}{\sqrt{3}-1} = \frac{1}{\sqrt{3}-1} \cdot \frac{\sqrt{3}+1}{\sqrt{3}+1} = \frac{\sqrt{3}+1}{2}$.

(2) $\frac{\sqrt{3}+1}{2} = 1 + (\frac{\sqrt{3}-1}{2})$ since the numerator $\sqrt{3}+1$ of $\frac{\sqrt{3}+1}{2}$ is between 2 and 3. Now we have a remainder $r_2 = \frac{\sqrt{3}-1}{2}$ which is different from the previous remainder $r_1 = \sqrt{3} - 1$, so we have to compute $\frac{1}{r_2} = \frac{2}{\sqrt{3}-1}$, namely $\frac{2}{\sqrt{3}-1} = \frac{2}{\sqrt{3}-1} \cdot \frac{\sqrt{3}+1}{\sqrt{3}+1} = \sqrt{3} + 1$.

(3) $\sqrt{3} + 1 = 2 + (\sqrt{3} - 1)$ since $\sqrt{3} + 1$ is between 2 and 3.

Now this remainder $r_3 = \sqrt{3} - 1$ is the same as r_1, so instead of the same step being repeated infinitely often, as happened for $\sqrt{2}$, the same two steps will repeat infinitely often. This means we get the continued fraction

$$\sqrt{3} = 1 + 1/1 + 1/2 + 1/1 + 1/2 + 1/1 + 1/2 + \cdots$$

Checking this takes a little more work than before. We begin by isolating the part of the continued fraction that repeats periodically, so we set

$$x = 1/1 + 1/2 + 1/1 + 1/2 + 1/1 + 1/2 + \cdots$$

Taking reciprocals, we get

$$\frac{1}{x} = 1 + 1/2 + 1/1 + 1/2 + 1/1 + 1/2 + \cdots$$

Subtracting 1 from both sides gives

$$\frac{1}{x} - 1 = 1/2 + 1/1 + 1/2 + 1/1 + 1/2 + \cdots$$

The next step will be to take reciprocals of both sides, so before doing this we rewrite the left side as $\frac{1-x}{x}$. Then taking reciprocals gives

$$\frac{x}{1-x} = 2 + 1/1 + 1/2 + 1/1 + 1/2 + \cdots$$

Hence

$$\frac{x}{1-x} - 2 = 1/1 + 1/2 + 1/1 + 1/2 + \cdots = x$$

Now we have the equation $\frac{x}{1-x} - 2 = x$ which can be simplified to the quadratic equation $x^2+2x-2=0$, with roots $x = -1 \pm \sqrt{3}$. Again the negative root is discarded, and we get $x = -1 + \sqrt{3}$. Thus $\sqrt{3} = 1 + x = 1 + 1/1 + 1/2 + 1/1 + 1/2 + 1/1 + 1/2 + \cdots$.

To simplify the notation we will write a bar over a block of terms in a continued fraction that repeat infinitely often, for example

$$\sqrt{2} = 1 + \overline{1/2} \qquad \text{and} \qquad \sqrt{3} = 1 + \overline{1/1 + 1/2}$$

It is true in general that for every positive integer n that is not a square, the continued fraction for $\sqrt{n}$ has the form $a_0 + \overline{1/a_1 + 1/a_2 + \cdots + 1/a_k}$. The length of the period can be large, for example

$$\sqrt{46} = 6 + \overline{1/1 + 1/3 + 1/1 + 1/1 + 1/2 + 1/6 + 1/2 + 1/1 + 1/1 + 1/3 + 1/1 + 1/12}$$

This example illustrates two other curious facts about the continued fraction for an irrational number $\sqrt{n}$:

(i) The last term of the period (12 in the example) is always twice the integer a_0 (the initial 6).

(ii) If the last term of the period is omitted, the preceding terms in the period form a palindrome, reading the same backwards as forwards.

We will see in Chapter 4 why these two properties have to be true.

It is natural to ask exactly which irrational numbers have continued fractions that are periodic, or at least *eventually* periodic, like for example

$$1/2 + 1/4 + \overline{1/3 + 1/5 + 1/7} = 1/2 + 1/4 + 1/3 + 1/5 + 1/7 + 1/3 + 1/5 + 1/7 + 1/3 + 1/5 + 1/7 + \cdots$$

The answer is given by a theorem of Lagrange from around 1766:

Lagrange's Theorem. *The irrational numbers whose continued fractions are eventually periodic are exactly the numbers of the form $a + b\sqrt{n}$ where a and b are rational numbers, $b \neq 0$, and n is a positive integer that is not a square.*

These numbers $a + b\sqrt{n}$ are called *quadratic irrationals* because they are roots of quadratic equations with integer coefficients. The easier half of the theorem is the statement that the value of an eventually periodic infinite continued fraction is always a quadratic irrational. This can be proved by showing that the method we used for finding a quadratic equation satisfied by an eventually periodic continued fraction works in general. Rather than following this purely algebraic approach, however, we will develop a more geometric version of the procedure in the next chapter, so we will wait until then to give the argument that proves this half of Lagrange's Theorem. The more difficult half of the theorem is the assertion that the continued fraction expansion of every quadratic irrational is eventually periodic. It is not at all apparent from the examples of $\sqrt{2}$ and $\sqrt{3}$ why this should be true in general, but in Chapter 5 we will develop some theory that will make it clear.

What can be said about the continued fraction expansions of irrational numbers that are not quadratic, such as $\sqrt[3]{2}$, π, or e, the base for natural logarithms? It happens that e has a continued fraction whose terms have a very nice pattern, even though they are not periodic or eventually periodic:

$$e = 2 + \underbrace{1/1 + 1/2 + 1/1}_{} + \underbrace{1/1 + 1/4 + 1/1}_{} + \underbrace{1/1 + 1/6 + 1/1}_{} + \cdots$$

where the terms are grouped by threes with successive even numbers as middle denominators. Even simpler are the continued fractions for certain numbers built from e that have arithmetic progressions for their denominators:

$$\frac{e-1}{e+1} = 1/2 + 1/6 + 1/10 + 1/14 + \cdots$$
$$\frac{e^2-1}{e^2+1} = 1/1 + 1/3 + 1/5 + 1/7 + \cdots$$

The continued fractions for e and $(e-1)/(e+1)$ were discovered by Euler in 1737 while the formula for $(e^2-1)/(e^2+1)$ was found by Lambert in 1766 as a special case of a slightly more complicated formula for $(e^x-1)/(e^x+1)$.

For $\sqrt[3]{2}$ and π, however, the continued fractions have no known pattern. For π the continued fraction begins

$$\pi = 3 + 1/7 + 1/15 + 1/1 + 1/292 + \cdots$$

Here the first four convergents are 3, $22/7$, $333/106$, and $355/113$. We recognize $22/7$ as the familiar approximation $3\frac{1}{7}$ to π. The convergent $355/113$ is a particularly good approximation to π since its decimal expansion begins 3.14159282 whereas $\pi = 3.1415926535\cdots$. It is no accident that the convergent $355/113$ obtained by truncating the continued fraction just before the 292 term gives a good approximation

to π since it is a general fact that a convergent immediately preceding a large term in the continued fraction always gives an especially good approximation, because the next jump in the zigzag path in the Farey diagram will be rather small, and all succeeding jumps will of course be smaller still.

There are nice continued fractions for π if one allows numerators larger than 1, as in the following formula discovered by Euler:

$$\pi = 3 + {}^{1^2}\!\nearrow_6 + {}^{3^2}\!\nearrow_6 + {}^{5^2}\!\nearrow_6 + {}^{7^2}\!\nearrow_6 + \cdots$$

However, it is the continued fractions with numerator 1 that have the nicest properties, so we will not consider the more general sort in this book.

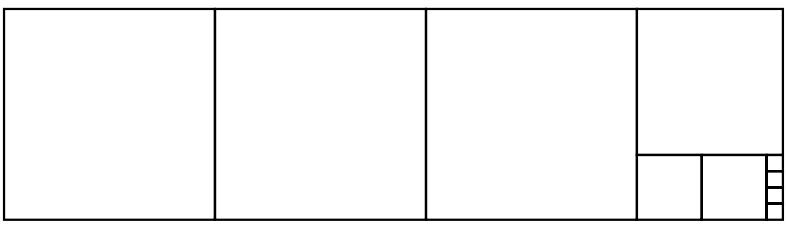
Exercises

1. (a) Compute the values of the continued fractions ${}^1\!\nearrow_1 + {}^1\!\nearrow_3 + {}^1\!\nearrow_5 + {}^1\!\nearrow_7$ and ${}^1\!\nearrow_1 + {}^1\!\nearrow_1 + {}^1\!\nearrow_1 + {}^1\!\nearrow_1 + {}^1\!\nearrow_1 + {}^1\!\nearrow_2$.
(b) Compute the continued fraction expansions of $19/44$ and $101/1020$.

2. (a) Compute the continued fraction for $38/83$ and display the steps of the Euclidean algorithm as a sequence of equations involving just integers.
(b) For the same number $38/83$ compute the associated strip of triangles (with large triangles subdivided into fans of smaller triangles), including the labeling of the vertices of all the triangles.
(c) Take the continued fraction ${}^1\!\nearrow_{a_1} + {}^1\!\nearrow_{a_2} + \cdots + {}^1\!\nearrow_{a_n}$ you got in part (a) and reverse the order of the numbers a_i to get a new continued fraction ${}^1\!\nearrow_{a_n} + {}^1\!\nearrow_{a_{n-1}} + \cdots + {}^1\!\nearrow_{a_1}$. Compute the value p/q of this continued fraction, and also compute the strip of triangles for this fraction p/q.

3. Let p_n/q_n be the value of the continued fraction ${}^1\!\nearrow_{a_1} + {}^1\!\nearrow_{a_2} + \cdots + {}^1\!\nearrow_{a_n}$ where each of the n terms a_i is equal to 2. For example, $p_1/q_1 = 1/2$ and $p_2/q_2 = {}^1\!\nearrow_2 + {}^1\!\nearrow_2 = 2/5$.
(a) Find equations expressing p_n and q_n in terms of p_{n-1} and q_{n-1}, and use these to write down the values of p_n/q_n for $n = 1, 2, 3, 4, 5, 6, 7$.
(b) Compute the strip of triangles for p_7/q_7.

4. (a) A rectangle whose sides have lengths 13 and 48 can be partitioned into squares in the following way:



Determine the lengths of the sides of all the squares, and relate the numbers of squares of each size to the continued fraction for $13/48$.

(b) Draw the analogous figure decomposing a rectangle of sides 19 and 42 into squares, and relate this to the continued fraction for $19/42$.

5. This exercise is intended to illustrate the proof of the first theorem in this chapter in the concrete case of the continued fraction $1/(2+1/(3+1/(4+1/5)))$.

(a) Write down the product $A_1A_2A_3A_4 = \begin{pmatrix}0&1\\1&a_1\end{pmatrix}\begin{pmatrix}0&1\\1&a_2\end{pmatrix}\begin{pmatrix}0&1\\1&a_3\end{pmatrix}\begin{pmatrix}0&1\\1&a_4\end{pmatrix}$ associated to $1/(2+1/(3+1/(4+1/5)))$.

(b) Compute the four matrices A_1, A_1A_2, $A_1A_2A_3$, $A_1A_2A_3A_4$ and relate these to the edges of the zigzag path in the strip of triangles for $1/(2+1/(3+1/(4+1/5)))$.

(c) Compute the four matrices A_4, A_3A_4, $A_2A_3A_4$, $A_1A_2A_3A_4$ and relate these to the successive fractions that one gets when one computes the value of $1/(2+1/(3+1/(4+1/5)))$, namely $1/5$, $1/(4+1/5)$, $1/(3+1/(4+1/5))$, and $1/(2+1/(3+1/(4+1/5)))$.

6. (a) Find all integer solutions of the equations $40x+89y=1$ and $40x+89y=5$.

(b) Find another equation $ax+by=1$ with integer coefficients a and b that has an integer solution in common with $40x+89y=1$. [Hint: use the Farey diagram.]

7. There is a close connection between the Diophantine equation $ax+by=n$ and the congruence $ax \equiv n \bmod b$, where the symbol $\equiv$ means "is congruent to". Namely, if one has a solution (x,y) to $ax+by=n$ then $ax \equiv n \bmod b$, and conversely, if one has a number x such that $ax \equiv n \bmod b$ then this means that $ax-n$ is a multiple of b, say k times b, so $ax-n=kb$ or equivalently $ax-kb=n$ so one has a solution of $ax+by=n$ with $y=-k$.

Using this viewpoint, find all integers x satisfying the congruence $31x \equiv 1 \bmod 71$, and then do the same for the congruence $31x \equiv 10 \bmod 71$. Are the solutions unique mod 71, i.e., unique up to adding multiples of 71?

8. Compute the values of the following infinite continued fractions:

(a) $\overline{1/4}$

(b) $\overline{1/k}$ for an arbitrary positive integer k.

(c) $\overline{1/(2+1/3)}$ and $1/(1+\overline{1/(2+1/3)})$

(d) $\overline{1/(1+1/(2+1/(1+1/6)))}$ and $1/(1+1/(4+\overline{1/(1+1/(2+1/(1+1/6)))}))$

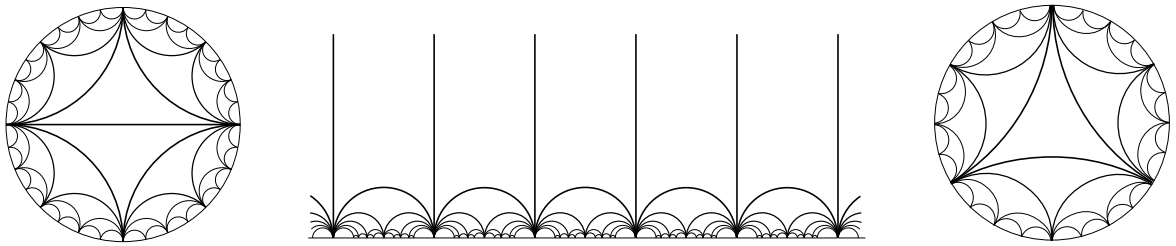
(e) $\overline{1/(2+1/(3+1/5))}$

9. Compute the continued fractions for $\sqrt{5}$ and $\sqrt{23}$.

10. Compute the continued fractions for $\sqrt{n^2+1}$ and $\sqrt{n^2+n}$ where n is an arbitrary positive integer.

Chapter 3. Linear Fractional Transformations

One thing one notices about the various versions of the Farey diagram is their symmetry. For the circular Farey diagram the symmetries are the reflections across the horizontal and vertical axes and the 180 degree rotation about the center. For the standard Farey diagram in the upper halfplane there are symmetries that translate the diagram by any integer distance to the left or the right, as well as reflections across certain vertical lines, the vertical lines through an integer or half-integer point on the x-axis. The Farey diagram could also be drawn to have 120 degree rotational symmetry and three reflectional symmetries.



Our purpose in this chapter is to study all possible symmetries of the Farey diagram, where we interpret the word "symmetry" in a broader sense than the familiar meaning from Euclidean geometry. For our purposes, symmetries will be invertible transformations that take vertices to vertices and edges to edges. (It follows that triangles are sent to triangles.) There are simple algebraic formulas for these more general symmetries, and these formulas lead to effective means of calculation. One of the applications will be to computing the values of periodic or eventually periodic continued fractions.

From linear algebra one is familiar with the way in which 2×2 matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ correspond to linear transformations of the plane $\mathbb{R}^2$, transformations of the form

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$$

In our situation we are going to restrict a, b, c, d, x, y to be integers. Then by associating to a pair (x, y) the fraction x/y one obtains a closely related transformation

$$T\left(\frac{x}{y}\right) = \frac{ax+by}{cx+dy} = \frac{a(\frac{x}{y})+b}{c(\frac{x}{y})+d}$$

If we set $z = x/y$ then T can also be written in the form

$$T(z) = \frac{az+b}{cz+d}$$

Such a transformation is called a *linear fractional transformation* since it is defined by a fraction whose numerator and denominator are linear functions.

In the formula $T(x/y) = (ax+by)/(cx+dy)$ there is no problem with allowing $x/y = 1/0$ just by setting $(x, y) = (1, 0)$, and the result is that $T(1/0) = a/c$. The value $T(x/y) = (ax+by)/(cx+dy)$ can also sometimes be $1/0$. This means

that T defines a function from vertices of the Farey diagram to vertices of the Farey diagram. We would like T to take edges of the diagram to edges of the diagram, and the following result gives a condition for this to happen.

Proposition. *If the matrix* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *has determinant* ± 1 *then the associated linear fractional transformation* T *takes each pair of vertices in the Farey diagram that lie at the ends of an edge of the diagram to another such pair of vertices.*

Proof: We showed in Chapter 1 that two vertices labeled p/q and r/s are joined by an edge in the diagram exactly when $ps - qr = \pm 1$, or in other words when the matrix $\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$ has determinant ± 1. The two columns of the product matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$ correspond to the two vertices $T(p/q)$ and $T(r/s)$, by the definition of matrix multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix} = \begin{pmatrix} ap+bq & ar+bs \\ cp+dq & cr+ds \end{pmatrix}$$

The proposition can then be restated as saying that if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$ each have determinant ± 1 then so does their product $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$. But it is a general fact about determinants that the determinant of a product is the product of the determinants. (This is easy to prove by a direct calculation in the case of 2×2 matrices.) So the product of two matrices of determinant ± 1 has determinant ± 1. □

As notation, we will use $LF(\mathbb{Z})$ to denote the set of all linear fractional transformations $T(x/y) = (ax+by)/(cx+dy)$ with coefficients a, b, c, d in $\mathbb{Z}$ such that the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has determinant ± 1.

Changing the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to its negative $\left(\begin{smallmatrix} -a & -b \\ -c & -d \end{smallmatrix}\right)$ produces the same linear fractional transformation since $(-ax-by)/(-cx-dy) = (ax+by)/(cx+dy)$. This is in fact the only way that different matrices can give the same linear fractional transformation T, as we will see later in this chapter. Note that changing $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to its negative $\left(\begin{smallmatrix} -a & -b \\ -c & -d \end{smallmatrix}\right)$ does not change the determinant. Thus each linear fractional transformation in $LF(\mathbb{Z})$ has a well-defined determinant, either $+1$ or -1. Later in this chapter we will also see how the distinction between determinant $+1$ and determinant -1 has a geometric interpretation in terms of orientations.

A useful fact about $LF(\mathbb{Z})$ is that each transformation T in $LF(\mathbb{Z})$ has an inverse T^{-1} in $LF(\mathbb{Z})$ because the inverse of a 2×2 matrix is given by the formula

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Thus if a, b, c, d are integers with $ad - bc = \pm 1$ then the inverse matrix also has integer entries and determinant ± 1. The factor $\frac{1}{ad-bc}$ is ± 1 so it can be ignored since the matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $-\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ determine the same linear fractional transformation, as we observed in the preceding paragraph.

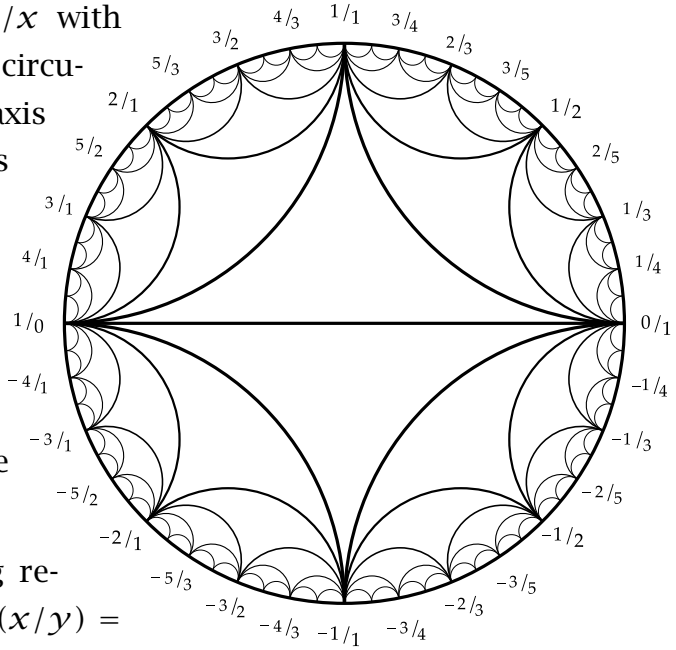
The preceding proposition says that each linear fractional transformation T in $LF(\mathbb{Z})$ not only sends vertices of the Farey diagram to vertices, but also edges to edges. It follows that T must take triangles in the diagram to triangles in the diagram, since triangles correspond to sets of three vertices, each pair of which forms the endpoints of an edge. Since each transformation T in $LF(\mathbb{Z})$ has an inverse in $LF(\mathbb{Z})$, this implies that T gives a one-to-one (injective) and onto (surjective) transformation of vertices, and also of edges and triangles. For example, if two edges e_1 and e_2 have the same image $T(e_1) = T(e_2)$ then we must have $T^{-1}(T(e_1)) = T^{-1}(T(e_2))$ or in other words $e_1 = e_2$, so T cannot send two different edges to the same edge, which means it is one-to-one on edges. Also, every edge e_1 is the image $T(e_2)$ of some edge e_2 since we can write $e_1 = T(T^{-1}(e_1))$ and let $e_2 = T^{-1}(e_1)$. The same reasoning works with vertices and triangles as well as edges.

A useful property of linear fractional transformations that we will use repeatedly is that the way an element of $LF(\mathbb{Z})$ acts on the Farey diagram is uniquely determined by where a single triangle is sent. This is because once one knows where one triangle goes, this uniquely determines where the three adjacent triangles go, and this in turn determines where the six new triangles adjacent to these three go, and so on.

Seven Types of Transformations

We will now give examples illustrating seven different ways that elements of $LF(\mathbb{Z})$ can act on the Farey diagram.

(1) The transformation $T(x/y) = y/x$ with matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ gives a reflection of the circular Farey diagram across its vertical axis of symmetry. This is a reflection across a line perpendicular to an edge of the diagram.



(2) The reflection across the horizontal axis of symmetry is the element $T(x/y) = -x/y$ with matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. This is a reflection across an edge of the diagram.

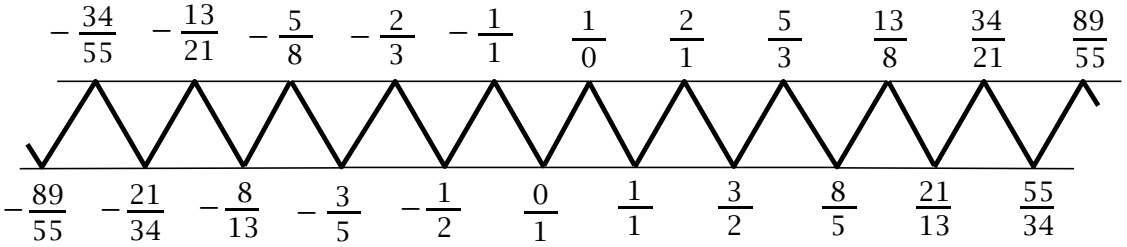
(3) If we compose the two preceding reflections we get the transformation $T(x/y) = -y/x$ with matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. This rotates the Farey diagram 180 degrees about its center, interchanging $1/0$ and $0/1$ and also interchanging $1/1$ and $-1/1$. Thus it rotates the diagram 180 degrees about the centerpoint of an edge.

(4) Consider $T(x/y) = y/(y-x)$ corresponding to the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)$. This has the effect of "rotating" the triangle $\langle 1/0, 0/1, 1/1\rangle$ about its centerpoint, taking $1/0$ to

$0/1$, $0/1$ to $1/1$ and $1/1$ back to $1/0$. The whole Farey diagram is then "rotated" about the same point.

(5) Next let $T(x/y) = x/(x+y)$, corresponding to the matrix $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$. In particular $T(0/1) = 0/1$, so $0/1$ is a fixed point of T, a point satisfying $T(z) = z$. Also we have $T(1/0) = 1/1$ and more generally $T(1/n) = 1/(n+1)$. Thus the triangle $\langle 0/1, 1/0, 1/1\rangle$ is taken to the triangle $\langle 0/1, 1/1, 1/2\rangle$. This implies that T is a "rotation" of the Farey diagram about the vertex $0/1$, taking each triangle with $0/1$ as a vertex to the next triangle in the clockwise direction about this vertex.

(6) A different sort of behavior is exhibited by $T(x/y) = (2x+y)/(x+y)$ corresponding to $\left(\begin{smallmatrix}2 & 1\\ 1 & 1\end{smallmatrix}\right)$. To visualize T as a transformation of the Farey diagram let us look at the infinite strip



We claim that T translates the whole strip one unit to the right. To see this, notice first that since T takes $1/0$ to $2/1$, $0/1$ to $1/1$, and $1/1$ to $3/2$, it takes the triangle $\langle 1/0, 0/1, 1/1\rangle$ to the triangle $\langle 2/1, 1/1, 3/2\rangle$. This implies that T takes the triangle just to the right of $\langle 1/0, 0/1, 1/1\rangle$ to the triangle just to the right of $\langle 2/1, 1/1, 3/2\rangle$, and similarly each successive triangle is translated one unit to the right. The same argument shows that each successive triangle to the left of the original one is also translated one unit to the right. Thus the whole strip is translated one unit to the right.

(7) Using the same figure as in the preceding example, consider the transformation $T(x/y) = (x+y)/x$ corresponding to the matrix $\left(\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right)$. This sends the triangle $\langle 1/0, 0/1, 1/1\rangle$ to $\langle 1/1, 1/0, 2/1\rangle$ which is the next triangle to the right in the infinite strip. Geometrically, T translates the first triangle half a unit to the right and reflects it across the horizontal axis of the strip. It follows that the whole strip is translated half a unit to the right and reflected across the horizontal axis. Such a motion is sometimes referred to as a glide-reflection. Notice that performing this motion twice in succession yields a translation of the strip one unit to the right, the transformation in the preceding example.

Thus we have seven types of symmetries of the Farey diagram: reflections across an edge or a line perpendicular to an edge; rotations about the centerpoint of an edge or a triangle, or about a vertex; and translations and glide-reflections of periodic infinite strips. (Not all periodic strips have glide-reflection symmetries.) It is a true fact, though we won't prove it here, that every element of $LF(\mathbb{Z})$ acts on the Farey

diagram in one of these seven ways, except for the identity transformation $T(x/y) = x/y$ of course.

Specifying Where a Triangle Goes

As we observed earlier, the action of an element of $LF(\mathbb{Z})$ on the Farey diagram is completely determined by where it sends a single triangle. Now we will see that there always exists an element of $LF(\mathbb{Z})$ sending any triangle to any other triangle, and in fact, one can do this specifying where each individual vertex of the triangle goes.

As an example, suppose we wish to find an element T of $LF(\mathbb{Z})$ that takes the triangle $\langle 2/5, 1/3, 3/8\rangle$ to the triangle $\langle 5/8, 7/11, 2/3\rangle$, preserving the indicated ordering of the vertices, so $T(2/5) = 5/8$, $T(1/3) = 7/11$, and $T(3/8) = 2/3$. For this problem to even make sense we might want to check first that these really are triangles in the Farey diagram. In the first case, $\langle 2/5, 1/3\rangle$ is an edge since the matrix $\left(\begin{smallmatrix} 2 & 1 \\ 5 & 3 \end{smallmatrix}\right)$ has determinant 1, and there is a triangle joining this edge to $3/8$ since $3/8$ is the mediant of $2/5$ and $1/3$. For the other triangle, the determinant of $\left(\begin{smallmatrix} 5 & 2 \\ 8 & 3 \end{smallmatrix}\right)$ is -1 and the mediant of $5/8$ and $2/3$ is $7/11$.

As a first step toward constructing the desired transformation T we will do something slightly weaker: We construct a transformation T taking the edge $\langle 2/5, 1/3\rangle$ to the edge $\langle 5/8, 7/11\rangle$. This is rather easy if we first notice the general fact that the transformation $T(x/y) = (ax + by)/(cx + dy)$ with matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ takes $1/0$ to a/c and $0/1$ to b/d. Thus the transformation T_1 with matrix $\left(\begin{smallmatrix} 2 & 1 \\ 5 & 3 \end{smallmatrix}\right)$ takes $\langle 1/0, 0/1\rangle$ to $\langle 2/5, 1/3\rangle$, and the transformation T_2 with matrix $\left(\begin{smallmatrix} 5 & 7 \\ 8 & 11 \end{smallmatrix}\right)$ takes $\langle 1/0, 0/1\rangle$ to $\langle 5/8, 7/11\rangle$. Then the product

$$T_2 T_1^{-1} = \begin{pmatrix} 5 & 7 \\ 8 & 11 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}^{-1}$$

takes $\langle 2/5, 1/3\rangle$ first to $\langle 1/0, 0/1\rangle$ and then to $\langle 5/8, 7/11\rangle$. Doing the calculation, we get

$$\begin{pmatrix} 5 & 7 \\ 8 & 11 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 5 & 7 \\ 8 & 11 \end{pmatrix} \begin{pmatrix} 3 & -1 \\ -5 & 2 \end{pmatrix} = \begin{pmatrix} -20 & 9 \\ -31 & 14 \end{pmatrix}$$

This takes the edge $\langle 2/5, 1/3\rangle$ to the edge $\langle 5/8, 7/11\rangle$, but does it do the right thing on the third vertex of the triangle $\langle 2/5, 1/3, 3/8\rangle$, taking it to the third vertex of $\langle 5/8, 7/11, 2/3\rangle$? This is not automatic since there are always two triangles containing a given edge, and in this case the other triangle having $\langle 5/8, 7/11\rangle$ as an edge is $\langle 5/8, 7/11, 12/19\rangle$ since $12/19$ is the mediant of $5/8$ and $7/11$. In fact, if we compute what our T does to $3/8$ we get

$$\begin{pmatrix} -20 & 9 \\ -31 & 14 \end{pmatrix} \begin{pmatrix} 3 \\ 8 \end{pmatrix} = \begin{pmatrix} 12 \\ 19 \end{pmatrix}$$

so we don't have the right T yet. To fix the problem, notice that we have a little flexibility in the choice of a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ taking $1/0$ to a/c and $0/1$ to b/d since

we can multiply either column by -1 without affecting the fractions a/b and c/d. It doesn't matter which column we multiply by -1 since multiplying both columns by -1 multiplies the whole matrix by -1 which doesn't change the associated element of $LF(\mathbb{Z})$, as noted earlier. In the case at hand, suppose we change the sign of the first column of $\left(\begin{smallmatrix} 5 & 7 \\ 8 & 11 \end{smallmatrix}\right)$. Then we get

$$\begin{pmatrix} -5 & 7 \\ -8 & 11 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} -5 & 7 \\ -8 & 11 \end{pmatrix}\begin{pmatrix} 3 & -1 \\ -5 & 2 \end{pmatrix} = \begin{pmatrix} -50 & 19 \\ -79 & 30 \end{pmatrix}$$

This fixes the problem since

$$\begin{pmatrix} -50 & 19 \\ -79 & 30 \end{pmatrix}\begin{pmatrix} 3 \\ 8 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

Here is a general statement summarizing what we saw in this one example:

Proposition. *(a) For any two triangles $\langle p/q, r/s, t/u\rangle$ and $\langle p'/q', r'/s', t'/u'\rangle$ in the Farey diagram there is a unique element T in $LF(\mathbb{Z})$ taking the first triangle to the second triangle preserving the ordering of the vertices, so $T(p/q) = p'/q'$, $T(r/s) = r'/s'$, and $T(t/u) = t'/u'$.*
(b) The matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ representing a given transformation T in $LF(\mathbb{Z})$ is unique except for replacing it by $\left(\begin{smallmatrix} -a & -b \\ -c & -d \end{smallmatrix}\right)$.

Proof: As we saw in the example above, there is a composition $T_2T_1^{-1}$ taking the edge $\langle p/q, r/s\rangle$ to $\langle p'/q', r'/s'\rangle$, where T_1 has matrix $\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$ and T_2 has matrix $\left(\begin{smallmatrix} p' & r' \\ q' & s' \end{smallmatrix}\right)$. If this composition $T_2T_1^{-1}$ does not take t/u to t'/u' we modify T_2 by changing the sign of one of its columns, say the first column. Thus we change $\left(\begin{smallmatrix} p' & r' \\ q' & s' \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} -p' & r' \\ -q' & s' \end{smallmatrix}\right)$, which equals the product $\left(\begin{smallmatrix} p' & r' \\ q' & s' \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. The matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ corresponds to the transformation $R(x/y) = -x/y$ reflecting the Farey diagram across the edge $\langle 1/0, 0/1\rangle$. Thus we are replacing $T_2T_1^{-1}$ by $T_2RT_1^{-1}$, inserting a reflection that interchanges the two triangles containing the edge $\langle 1/0, 0/1\rangle$. By inserting R we change where the composition $T_2T_1^{-1}$ sends the third vertex t/u of the triangle $\langle p/q, r/s, t/u\rangle$, so we can guarantee that t/u is taken to t'/u'. This proves part (a).

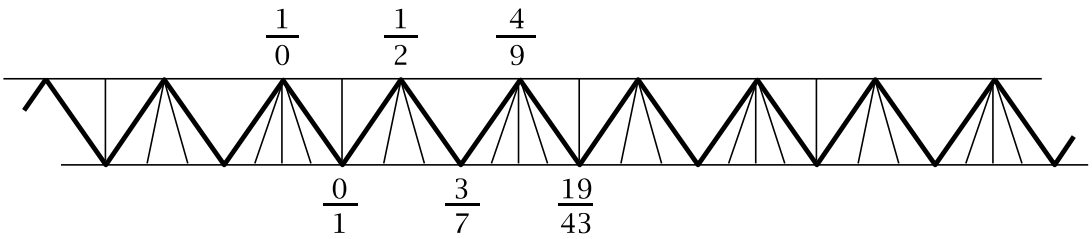
For part (b), note first that the transformation T determines the values $T(1/0) = a/c$ and $T(0/1) = b/d$. The fractions a/c and b/d are in lowest terms (because $ad - bc = \pm 1$) so this means that we know the two columns of the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ up to multiplying either or both columns by -1. We need to check that changing the sign of one column without changing the sign of the other column gives a different transformation. It doesn't matter which column we change since $\left(\begin{smallmatrix} -a & b \\ -c & d \end{smallmatrix}\right) = -\left(\begin{smallmatrix} a & -b \\ c & -d \end{smallmatrix}\right)$. As we saw in part (a), changing the sign in the first column amounts to replacing T by the composition TR, but this is a different transformation from T since it has a different effect on the triangles containing the edge $\langle 1/0, 0/1\rangle$. □

Continued Fractions Again

Linear fractional transformations can be used to compute the values of periodic or eventually periodic continued fractions, and to see that these values are always quadratic irrational numbers. To illustrate this, consider the periodic continued fraction

$$\overline{1/2 + 1/3 + 1/1 + 1/4}$$

The associated periodic strip in the Farey diagram is the following:



We would like to compute the element T of $LF(\mathbb{Z})$ that gives the rightward translation of this strip that exhibits the periodicity. A first guess is the T with matrix $\left(\begin{smallmatrix} 4 & 19 \\ 9 & 43 \end{smallmatrix}\right)$ since this sends $\langle 1/0, 0/1\rangle$ to $\langle 4/9, 19/43\rangle$. This is actually the correct T since it sends the vertex $1/1$ just to the right of $1/0$, which is the mediant of $1/0$ and $0/1$, to the vertex $(4+19)/(9+43)$ just to the right of $4/9$, which is the mediant of $4/9$ and $19/43$. This is a general fact since $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a+b \\ c+d \end{smallmatrix}\right)$.

The sequence of fractions labeling the vertices along the zigzag path in the strip moving toward the right are the convergents to $\overline{1/2 + 1/3 + 1/1 + 1/4}$. Call these convergents $z_1, z_2, \cdots$ and their limit z. When we apply the translation T we are taking each convergent to a later convergent in the sequence, so both the sequence $\{z_n\}$ and the sequence $\{T(z_n)\}$ converge to z. Thus we have

$$T(z) = T(\lim z_n) = \lim T(z_n) = z$$

where the middle equality uses the fact that T is continuous. (Note that a linear fractional transformation $T(z) = \frac{az+b}{cz+d}$ is defined for real values of z, not just rational values $z = x/y$, when $T(x/y) = (ax+by)/(cx+dy) = (a\frac{x}{y} + b)/(c\frac{x}{y} + d)$.)

In summary, what we have just argued is that the value z of the periodic continued fraction satisfies the equation $T(z) = z$, or in other words, $\frac{4z+19}{9z+43} = z$. This can be rewritten as $4z + 19 = 9z^2 + 43z$, which simplifies to $9z^2 + 39z - 19 = 0$. Computing the roots of this quadratic equation, we get

$$z = \frac{-39 \pm \sqrt{39^2 + 4 \cdot 9 \cdot 19}}{18} = \frac{-39 \pm 3\sqrt{13^2 + 4 \cdot 19}}{18} = \frac{-13 \pm \sqrt{245}}{6} = \frac{-13 \pm 7\sqrt{5}}{6}$$

The positive root is the one that the right half of the infinite strip converges to, so we have

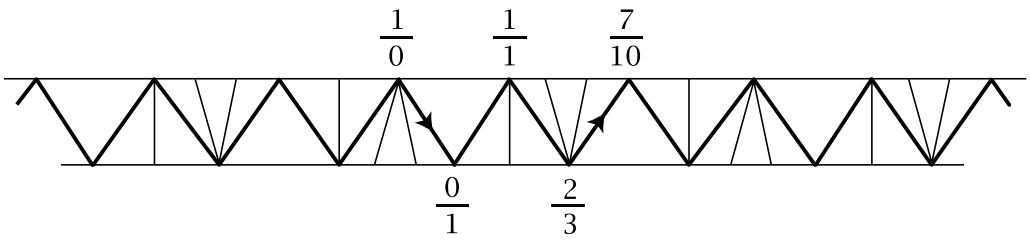
$$\frac{-13 + 7\sqrt{5}}{6} = \overline{1/2 + 1/3 + 1/1 + 1/4}$$

Incidentally, the other root $(-13-7\sqrt{5})/6$ has an interpretation in terms of the diagram as well: It is the limit of the numbers labeling the vertices of the zigzag path moving off to the left rather than to the right. This follows by the same sort of argument as above.

If a periodic continued fraction has period of odd length, the transformation giving the periodicity is a glide-reflection of the periodic strip rather than a translation. As an example, consider

$$\overline{1\big/1+1\big/2+1\big/3}$$

Here the periodic strip is



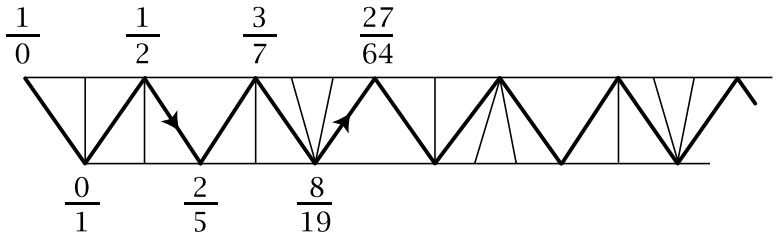
The transformation T with matrix $\left(\begin{smallmatrix}2 & 7\\ 3 & 10\end{smallmatrix}\right)$ takes $\langle 1/0, 0/1\rangle$ to $\langle 2/3, 7/10\rangle$ and the mediant $1/1$ of $1/0$ and $0/1$ to the mediant $9/13$ of $2/3$ and $7/10$ so this transformation is a glide-reflection of the strip. The equation $T(z)=z$ becomes $\frac{2z+7}{3z+10}=z$, which simplifies to $2z+7=3z^2+10z$ and then $3z^2+8z-7=0$, with roots $(-4\pm\sqrt{37})/3$. The positive root gives

$$\frac{-4+\sqrt{37}}{3}=\overline{1\big/1+1\big/2+1\big/3}$$

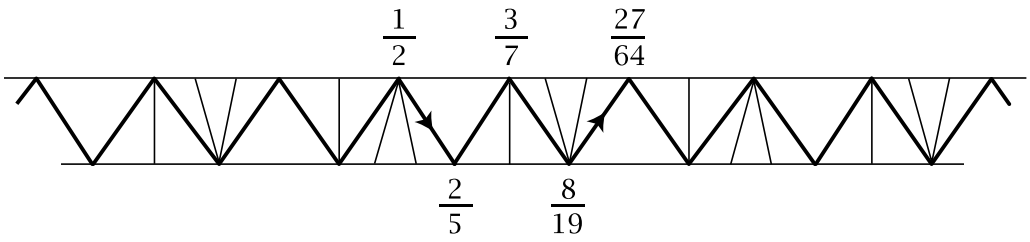
Continued fractions that are only eventually periodic can be treated in a similar fashion. For example, consider

$$1\big/2+1\big/2+\overline{1\big/1+1\big/2+1\big/3}$$

The corresponding infinite strip is



In this case if we discard the triangles corresponding to the initial nonperiodic part of the continued fraction, $1/2+1/2$, and then extend the remaining periodic part in both directions, we obtain a periodic strip that is carried to itself by the glide-reflection T taking $\langle 1/2, 2/5\rangle$ to $\langle 8/19, 27/64\rangle$:



We can compute T as the composition $\langle 1/2, 2/5\rangle \to \langle 1/0, 0/1\rangle \to \langle 8/19, 27/64\rangle$ corresponding to the product

$$\begin{pmatrix} 8 & 27 \\ 19 & 64 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 8 & 27 \\ 19 & 64 \end{pmatrix}\begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} -14 & 11 \\ -33 & 26 \end{pmatrix}$$

Since this transformation takes $3/7$ to the mediant $(8+27)/(19+64)$, it is the glide-reflection we want. Now we solve $T(z) = z$. This means $\frac{-14z+11}{-33z+26} = z$, which reduces to the equation $33z^2 - 40z + 11 = 0$ with roots $z = (20 \pm \sqrt{37})/33$. Both roots are positive, and we want the smaller one, $(20 - \sqrt{37})/33$, because along the top edge of the strip the numbers decrease as we move to the right, approaching the smaller root, and they increase as we move to the left, approaching the larger root. Thus we have

$$(20 - \sqrt{37})/33 = 1/2 + 1/2 + \overline{1/1 + 1/2 + 1/3}$$

Notice that $\sqrt{37}$ occurs in both this example and the preceding one where we computed the value of $\overline{1/1 + 1/2 + 1/3}$. This is not just an accident. It had to happen because to get from $\overline{1/1 + 1/2 + 1/3}$ to $1/2 + 1/2 + \overline{1/1 + 1/2 + 1/3}$ one adds 2 and inverts, then adds 2 and inverts again, and each of these operations of adding an integer or taking the reciprocal takes place within the field $\mathbb{Q}(\sqrt{37})$ consisting of numbers of the form $a + b\sqrt{37}$ with a and b rational. More generally, this argument shows that any eventually periodic continued fraction whose periodic part is $\overline{1/1 + 1/2 + 1/3}$ has as its value some number in the field $\mathbb{Q}(\sqrt{37})$. However, not all irrational numbers in this field have eventually periodic continued fractions with periodic part $\overline{1/1 + 1/2 + 1/3}$. For example, the continued fraction for $\sqrt{37}$ itself is $6 + \overline{1/12}$, with a different periodic part. (Check this by computing the value of this continued fraction.)

One Half of Lagrange's Theorem

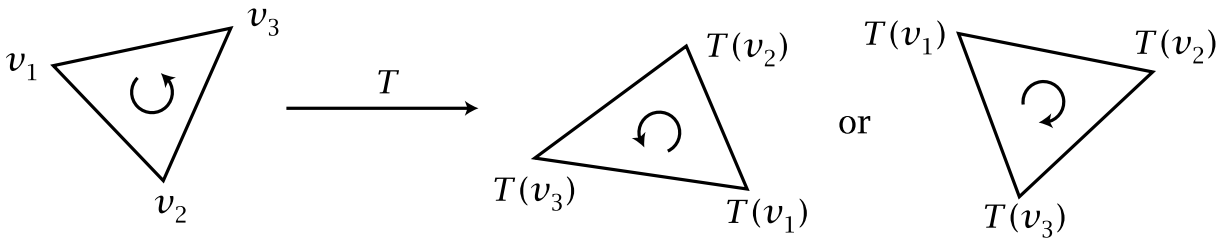
The procedure we have used in these examples works in general for any irrational number z whose continued fraction is eventually periodic. From the periodic part of the continued fraction one constructs a periodic infinite strip in the Farey diagram, where the periodicity is given by a linear fractional transformation $T(z) = \frac{az+b}{cz+d}$ with integer coefficients, with T either a translation or a glide-reflection of the strip. As we argued in the first example, the number z satisfies the equation $T(z) = z$. This becomes the quadratic equation $az + b = cz^2 + dz$ with integer coefficients, or in simpler form, $cz^2 + (d - a)z - b = 0$. By the quadratic formula, the roots of this equation have the form $A + B\sqrt{n}$ for some rational numbers A and B and some

integer n. We know that the real number z is a root of the equation so n can't be negative, and it can't be a square since z is irrational.

Thus we have an argument that proves one half of Lagrange's Theorem, the statement that a number whose continued fraction is periodic or eventually periodic is a quadratic irrational. There is one technical point that should be addressed, however. Could the leading coefficient c in the quadratic equation $cz^2 + (d-a)z - b = 0$ be zero? If this were the case then we couldn't apply the quadratic formula to solve for z, so we need to show that c cannot be zero. We do this in the following way. If c were zero the equation would become the linear equation $(d-a)z - b = 0$. If the coefficient of z in this equation is nonzero, we have only one root, $z = b/(d-a)$, a rational number contrary to the fact that z is irrational since its continued fraction is infinite. Thus we are left with the possibility that $c = 0$ and $a = d$, so the equation for z reduces to the equation $b = 0$. Then the transformation T would have the form $T(z) = \frac{az}{a} = z$ so it would be the identity transformation. However we know it is a genuine translation or a glide-reflection, so it is not the identity. We conclude from all this that c cannot be zero, and the technical point is taken care of.

Orientations

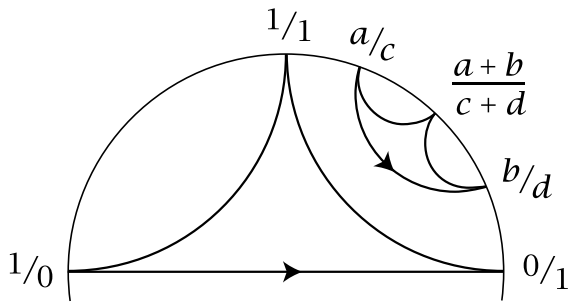
Elements of $LF(\mathbb{Z})$ are represented by integer matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ of determinant ± 1. The distinction between determinant $+1$ and -1 has a very nice geometric interpretation in terms of orientations, which can be described in terms of triangles. A triangle in the Farey diagram can be oriented by choosing either the clockwise or counterclockwise ordering of its three vertices. An element T of $LF(\mathbb{Z})$ takes each triangle to another triangle in a way that either preserves the two possible orientations or reverses them.



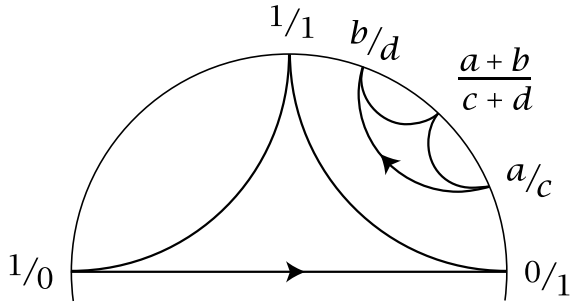
For example, among the seven types of transformations we looked at earlier, only reflections and glide-reflections reverse the orientations of triangles. Note that if a transformation T preserves the orientation of one triangle, it has to preserve the orientation of the three adjacent triangles, and then of the triangles adjacent to these, and so on for all the triangles. Similarly, if the orientation of one triangle is reversed by T, then the orientations of all triangles are reversed.

Proposition. *A transformation $T(x/y) = (ax + by)/(cx + dy)$ in $LF(\mathbb{Z})$ preserves orientations of triangles in the Farey diagram when the determinant $ad - bc$ is $+1$ and reverses the orientations when the determinant is -1.*

Proof: We will first prove a special case and then deduce the general case from the special case. The special case is that a, b, c, d are all positive or zero. The transformation T with matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ takes the edge $\langle 1/0, 0/1\rangle$ in the circular Farey diagram to the edge $\langle a/c, b/d\rangle$, and if a, b, c, d are all positive or zero, this edge lies in the upper half of the diagram. Since $T(1/1) = (a+b)/(c+d)$, the triangle $\langle 1/0, 0/1, 1/1\rangle$ is taken to the triangle $\langle a/c, b/d, (a+b)/(c+d)\rangle$ whose third vertex $(a+b)/(c+d)$ lies above the edge $\langle a/c, b/d\rangle$, by the way the Farey diagram was constructed using mediants, since we assume a, b, c, d are positive or zero. We know that the edge $\langle a/c, b/d\rangle$ is oriented to the right if $ad - bc = +1$ and to the left if $ad - bc = -1$. This means that T preserves the orientation of the triangle $\langle 1/0, 0/1, 1/1\rangle$ if the determinant is $+1$ and reverses the orientation if the determinant is -1.



$ad - bc = +1$



$ad - bc = -1$

This proves the special case.

The general case can be broken into two subcases, according to whether the edge $\langle a/c, b/d\rangle$ lies in the upper or the lower half of the diagram. If $\langle a/c, b/d\rangle$ lies in the upper half of the diagram, then after multiplying one or both columns of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ by -1 if necessary, we will be in the special case already considered. Multiplying both columns by -1 doesn't affect T. Multiplying one column by -1 corresponds to first reflecting across the edge $\langle 1/0, 0/1\rangle$, as we have seen earlier. Modifying T in this way changes the sign of the determinant and it also changes whether T preserves or reverses orientation, so the special case already proved implies the case that T takes $\langle 1/0, 0/1\rangle$ to an edge in the upper half of the diagram.

The remaining possibility is that T takes the edge $\langle 1/0, 0/1\rangle$ to an edge in the lower half of the diagram. In this case if we follow T by reflection across the edge $\langle 1/0, 0/1\rangle$ we get a new transformation taking $\langle 1/0, 0/1\rangle$ to an edge in the upper half of the diagram. As before, composing with this reflection changes T from orientation-preserving to orientation-reversing and vice versa, and it also changes the sign of the determinant since the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is changed to $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} -a & -b \\ c & d \end{smallmatrix}\right)$, so this case follows from the previous case. □

Computational note: To determine whether a matrix representing an element of $LF(\mathbb{Z})$ has determinant $+1$ or -1 it suffices to compute just the last digit of the

determinant, and this can be done using just the last digit of the entries in the matrix. This is easy to do in one's head even if the entries in the matrix have many digits.

We will let $LF^+(\mathbb{Z})$ denote the elements of $LF(\mathbb{Z})$ corresponding to matrices of determinant $+1$.

Proposition. *For any two edges $\langle p/q, r/s\rangle$ and $\langle p'/q', r'/s'\rangle$ of the Farey diagram there exists a unique element $T \in LF^+(\mathbb{Z})$ taking the first edge to the second edge preserving the ordering of the vertices, so $T(p/q) = p'/q'$ and $T(r/s) = r'/s'$.*

Proof: We already know that there exists an element T in $LF(\mathbb{Z})$ with $T(p/q) = p'/q'$ and $T(r/s) = r'/s'$, and in fact there are exactly two choices for T which are distinguished by which of the two triangles containing $\langle p'/q', r'/s'\rangle$ a triangle containing $\langle p/q, r/s\rangle$ is sent to. One of these choices will make T preserve orientation and the other will make T reverse orientation. So there is only one choice where the determinant is $+1$. □

Exercises

1. Find a formula for the linear fractional transformation that rotates the triangle $\langle 0/1, 1/2, 1/1\rangle$ to $\langle 1/1, 0/1, 1/2\rangle$.

2. Find the linear fractional transformation that reflects the Farey diagram across the edge $\langle 1/2, 1/3\rangle$ (so in particular, the transformation takes $1/2$ to $1/2$ and $1/3$ to $1/3$).

3. Find a formula for the linear fractional transformation that reflects the upper half-plane version of the Farey diagram across the vertical line $x = 3/2$.

4. Find an infinite periodic strip of triangles in the Farey diagram such that the transformation $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 2 \end{smallmatrix}\right)$ is a glide-reflection along this strip and the transformation $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 2 \\ 2 & 5 \end{smallmatrix}\right)$ is a translation along this strip.

5. Let T be an element of $LF(\mathbb{Z})$ with matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Show that the composition $T\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)T^{-1}$ is the reflection across the edge $\langle a/c, b/d\rangle = T(\langle 1/0, 0/1\rangle)$.

For each of the remaining six problems, compute the value of the given periodic or eventually periodic continued fraction by first drawing the associated infinite strip of triangles, then finding a linear fractional transformation T in $LF(\mathbb{Z})$ that gives the periodicity in the strip, then solving $T(z) = z$.

6. $\overline{1/2 + 1/5}$

7. $\overline{1/2 + 1/1 + 1/1}$

8. $\overline{1/1 + 1/1 + 1/1 + 1/1 + 1/1 + 1/2}$

9. $2 + \overline{1/1 + 1/1 + 1/4}$

10. $2 + \overline{1/1 + 1/1 + 1/1 + 1/4}$

11. $1/1 + 1/1 + \overline{1/2 + 1/3}$

Chapter 4. Quadratic Forms

Finding Pythagorean triples is answering the question, *When is the sum of two squares equal to a square*? More generally one can ask, *Exactly which numbers are sums of two squares*? In other words, when does an equation $x^2 + y^2 = n$ have integer solutions, and how can one find these solutions? The brute force approach of simply plugging in values for x and y leads to the following list of all solutions for $n \le 50$ (apart from interchanging x and y):

$$\mathbf{1} = 1^2 + 0^2,\ \mathbf{2} = 1^2 + 1^2,\ \mathbf{4} = 2^2 + 0^2,\ \mathbf{5} = 2^2 + 1^2,\ \mathbf{8} = 2^2 + 2^2,\ \mathbf{9} = 3^2 + 0^2,$$
$$\mathbf{10} = 3^2 + 1^2,\ \mathbf{13} = 3^2 + 2^2,\ \mathbf{16} = 4^2 + 0^2,\ \mathbf{17} = 4^2 + 1^2,\ \mathbf{18} = 3^2 + 3^2,$$
$$\mathbf{20} = 4^2 + 2^2,\ \mathbf{25} = 5^2 + 0^2 = 4^2 + 3^2,\ \mathbf{26} = 5^2 + 1^2,\ \mathbf{29} = 5^2 + 2^2,\ \mathbf{32} = 4^2 + 4^2,$$
$$\mathbf{34} = 5^2 + 3^2,\ \mathbf{36} = 6^2 + 0^2,\ \mathbf{37} = 6^2 + 1^2,\ \mathbf{40} = 6^2 + 2^2,\ \mathbf{41} = 5^2 + 4^2,$$
$$\mathbf{45} = 6^2 + 3^2,\ \mathbf{49} = 7^2 + 0^2,\ \mathbf{50} = 5^2 + 5^2 = 7^2 + 1^2$$

Notice that in some cases there is more than one solution for a given value of n. Our first goal will be to describe a more efficient way to find the integer solutions of $x^2 + y^2 = n$ and to display them graphically in a way that sheds much light on their structure. The technique for doing this will work not just for the function $x^2 + y^2$ but also for any function $Q(x, y) = ax^2 + bxy + cy^2$, where a, b, and c are integer constants. Such a function $Q(x, y)$ is called a *quadratic form*, or sometimes just a *form* for short.

Solving $x^2 + y^2 = n$ amounts to representing n in the form of the sum of two squares. More generally, solving $Q(x, y) = n$ is called *representing n by the form $Q(x, y)$*. So the overall goal is to solve the representation problem: Which numbers n are represented by a given form $Q(x, y)$, and how does one find such representations.

Before starting to describe the method for displaying the values of a quadratic form graphically let us make a preliminary observation:

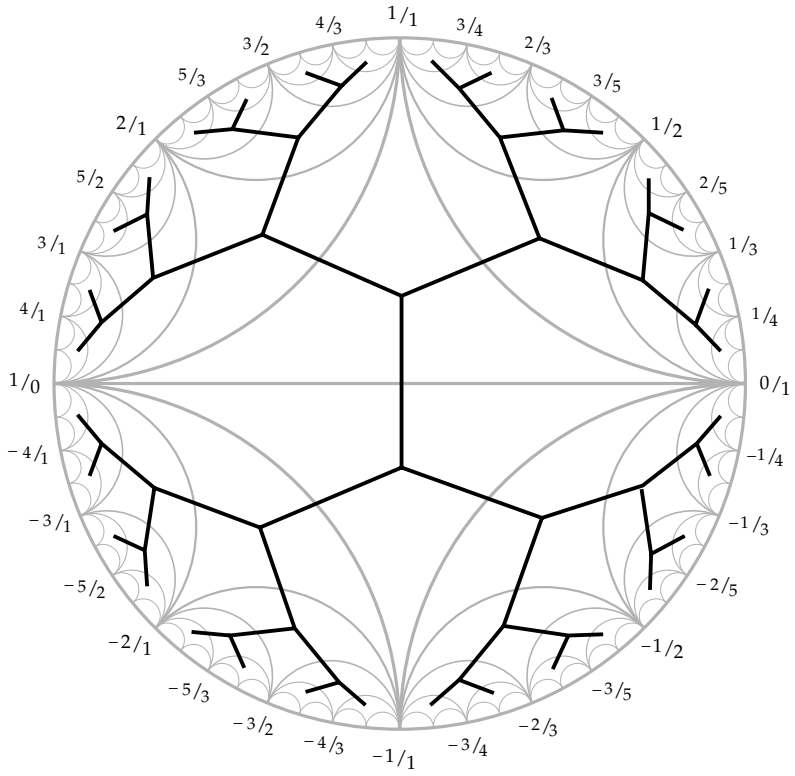
> If the greatest common divisor of two integers x and y is d, then $Q(x, y) = d^2 Q(\frac{x}{d}, \frac{y}{d})$ where the greatest common divisor of $\frac{x}{d}$ and $\frac{y}{d}$ is 1. Hence it suffices to find the values of Q on *primitive* pairs (x, y), the pairs whose greatest common divisor is 1, and then multiply these values by arbitrary squares d^2.

Thus the real problem is to find the primitive representations of a number n by a form $Q(x, y)$, or in other words, to find the primitive solutions of $Q(x, y) = n$.

Primitive pairs (x, y) correspond almost exactly to fractions x/y that are reduced to lowest terms, the only ambiguity being that both (x, y) and $(-x, -y)$ correspond to the same fraction x/y. However, this ambiguity does not affect the value of a quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ since $Q(x, y) = Q(-x, -y)$. This means that we can regard $Q(x, y)$ as being essentially a function $f(x/y)$. Notice that we are not excluding the possibility $(x, y) = (1, 0)$ which corresponds to the "fraction" $1/0$.

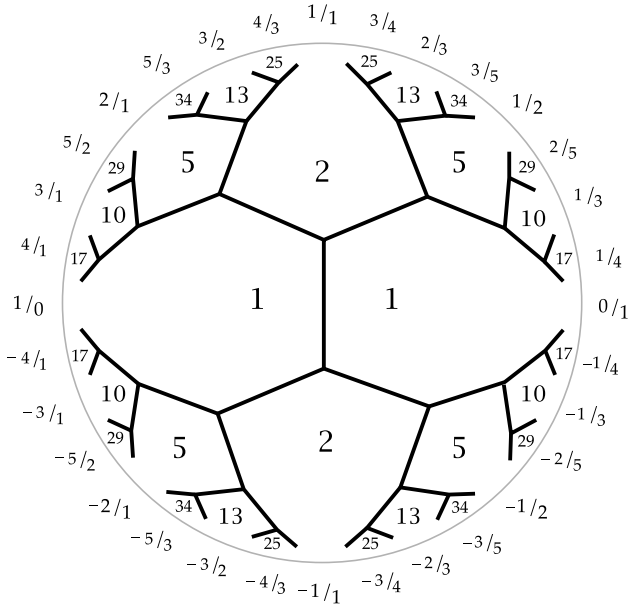
The Topograph

We already have a nice graphical representation of the rational numbers x/y and $1/0$ as the vertices in the Farey diagram. Here is a picture of the diagram with the so-called *dual tree* superimposed:



The dual tree has a vertex in the center of each triangle of the Farey diagram, and it has an edge crossing each edge of the Farey diagram. The upper half of the dual tree does actually look like a real tree, with the lower half being its reflection in still water. As with the Farey diagram, we can only draw a finite part of the dual tree. The actual dual tree has branching that repeats infinitely often, an unending bifurcation process with smaller and smaller twigs.

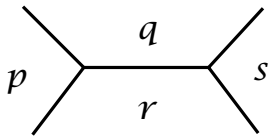
The tree divides the interior of the large circle into regions, each of which is adjacent to one vertex of the original diagram. We can write the value $Q(x, y)$ in the region adjacent to the vertex x/y. This is shown in the figure below for the quadratic form $Q(x, y) = x^2 + y^2$, where to unclutter the picture we no longer draw the triangles of the original Farey diagram.



For example the 13 in the region adjacent to the fraction $2/3$ represents the value $2^2 + 3^2$, and the 29 in the region adjacent to $5/2$ represents the value $5^2 + 2^2$.

For a quadratic form Q this picture showing the values $Q(x, y)$ is called the *topograph* of Q. It turns out that there is a very simple method for computing the topograph from just a very small amount of initial data. This method is based on the following:

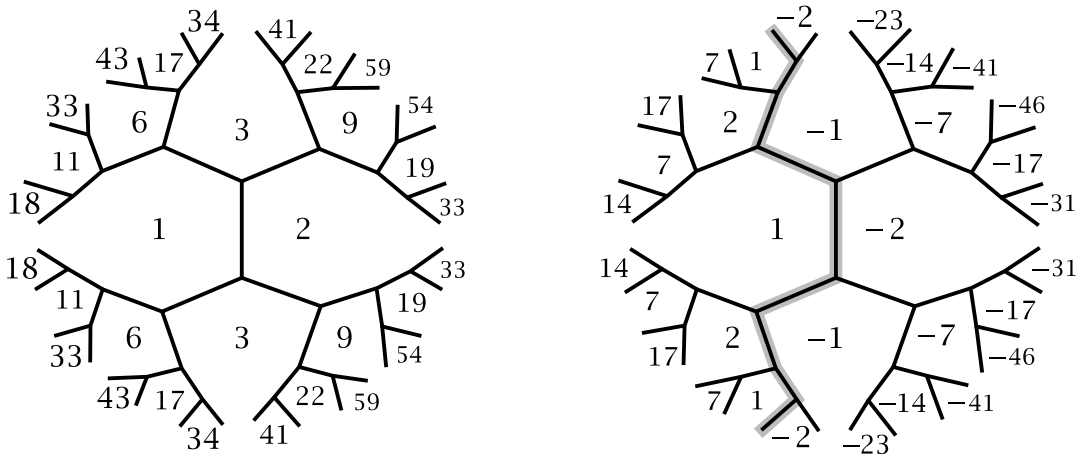
Arithmetic Progression Rule. If the values of $Q(x, y)$ in the four regions surrounding an edge in the tree are p, q, r, and s as indicated in the figure, then the three numbers p, $q + r$, s form an arithmetic progression.



We can check this in the topograph of $x^2 + y^2$ shown above. Consider for example one of the edges separating the values 1 and 2. The values in the four regions surrounding this edge are $1, 1, 2, 5$ and the arithmetic progression is $1, 1 + 2, 5$. For an edge separating the values 1 and 5 the arithmetic progression is $2, 1 + 5, 10$. For an edge separating the values 5 and 13 the arithmetic progression is $2, 5 + 13, 34$. And similarly for all the other edges.

The arithmetic progression rule implies that the values of Q in the three regions surrounding a single vertex of the tree determine the values in all other regions, by starting at the vertex where the three adjacent values are known and working one's way outward in the dual tree. The easiest place to start for a quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ is with the three values $Q(1, 0) = a$, $Q(0, 1) = c$, and $Q(1, 1) = a + b + c$ for the three fractions $1/0$, $0/1$, and $1/1$. Here are two examples:

$Q(x,y) = x^2 + 2y^2$ $Q(x,y) = x^2 - 2y^2$



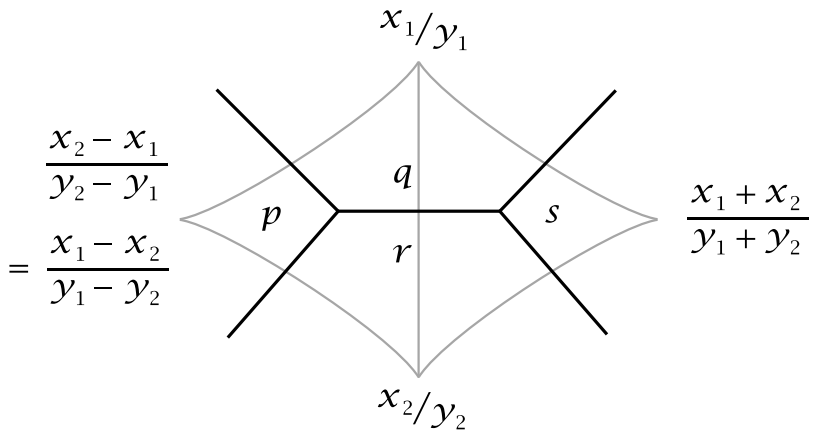
In the first case we start with the values 1 and 2 together with the 3 just above them. These determine the value 9 above the 2 via the arithmetic progression $1, 2+3, 9$. Similarly the 6 above the 1 is determined by the arithmetic progression $2, 1+3, 6$. Next one can fill in the 19 next to the 9 we just computed, using the arithmetic progression $3, 2+9, 19$, and so on for as long as one likes.

The procedure for the other form $x^2 - 2y^2$ is just the same, but here there are negative as well as positive values. The edges that separate positive values from negative values will be important later, so we have indicated these edges by special shading.

Perhaps the most noticeable thing in both the examples $x^2 + 2y^2$ and $x^2 - 2y^2$ is the fact that the values in the lower half of the topograph are the same as those in the upper half. We could have predicted in advance that this would happen because $Q(x,y) = Q(-x,y)$ whenever $Q(x,y)$ has the form $ax^2 + cy^2$, with no xy term. The topograph for $x^2 + y^2$ has even more symmetry since the values of $x^2 + y^2$ are unchanged when x and y are switched, so the topograph has left-right symmetry as well.

Here is a general observation: The three values around one vertex of the topograph can be specified arbitrarily. For if we are given three numbers a, b, c then the quadratic form $ax^2 + (c-a-b)xy + by^2$ takes these three values for (x,y) equal to $(1,0), (0,1), (1,1)$.

Proof of the Arithmetic Progression Rule: Let the two vertices of the Farey diagram corresponding to the values q and r have labels x_1/y_1 and x_2/y_2 as in the figure below. Then by the mediant rule for labeling vertices, the labels on the p and s regions are the fractions shown. Note that these labels are correct even when $x_1/y_1 = 1/0$ and $x_2/y_2 = 0/1$.



For a quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ we then have

$$\begin{aligned} s = Q(x_1 + x_2, y_1 + y_2) &= a(x_1 + x_2)^2 + b(x_1 + x_2)(y_1 + y_2) + c(y_1 + y_2)^2 \\ &= \underbrace{ax_1^2 + bx_1y_1 + cy_1^2}_{Q(x_1,y_1) = q} + \underbrace{ax_2^2 + bx_2y_2 + cy_2^2}_{Q(x_2,y_2) = r} + (\cdots) \end{aligned}$$

Similarly we have

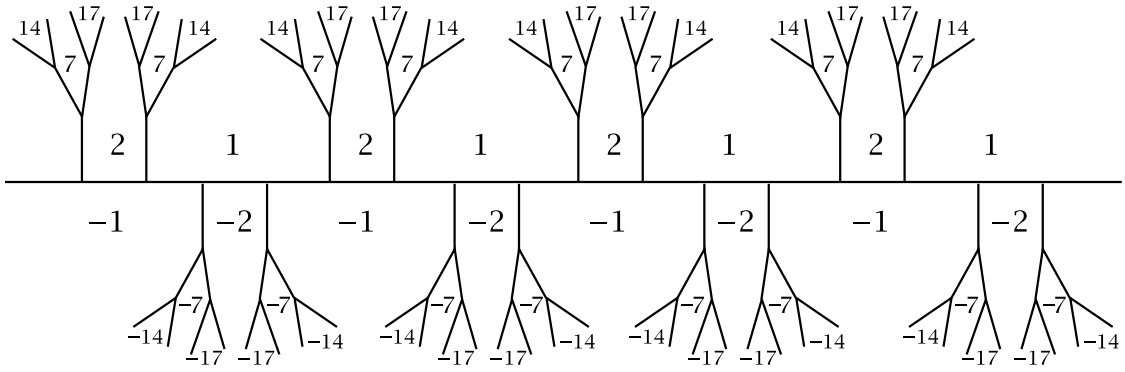
$$p = Q(x_1 - x_2, y_1 - y_2) = \underbrace{ax_1^2 + bx_1y_1 + cy_1^2}_{Q(x_1,y_1) = q} + \underbrace{ax_2^2 + bx_2y_2 + cy_2^2}_{Q(x_2,y_2) = r} - (\cdots)$$

The terms in $(\cdots)$ are the same in both cases, namely the terms involving both subscripts 1 and 2. If we compute $p + s$ by adding the two formulas together, the terms $(\cdots)$ will therefore cancel, leaving just $p + s = 2(q + r)$. This equation can be rewritten as $(q + r) - p = s - (q + r)$, which just says that $p, q + r, s$ forms an arithmetic progression. □

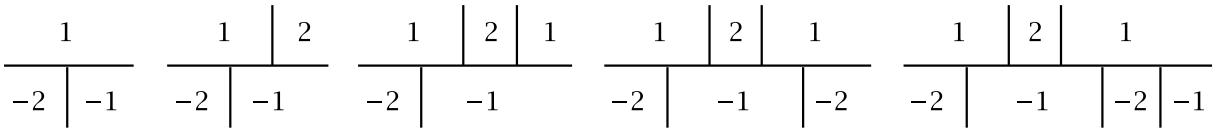
Periodic Separator Lines

For most quadratic forms that take on both positive and negative values, such as $x^2 - 2y^2$, there is another way of drawing the topograph that reveals some hidden and unexpected properties. For the form $x^2 - 2y^2$ there is a zigzag path of edges in the topograph separating the positive and negative values, and if we straighten this path out to be a line, called the *separator line*, what we see is the following infinitely repeated pattern:

$Q(x, y) = x^2 - 2y^2$

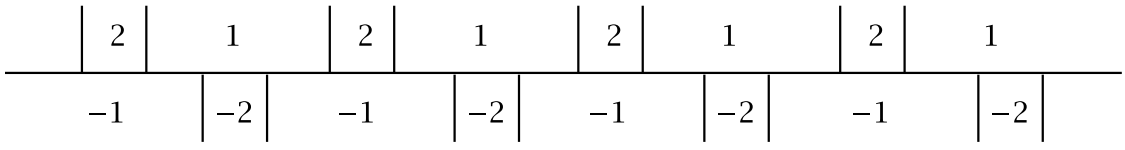


To construct this, one can first build the separator line starting with the three values $Q(1,0) = 1$, $Q(0,1) = -2$, and $Q(1,1) = -1$. Place these as shown in part (a) of the figure below, with a horizontal line segment separating the positive from the negative values.



(a) (b) (c) (d) (e)

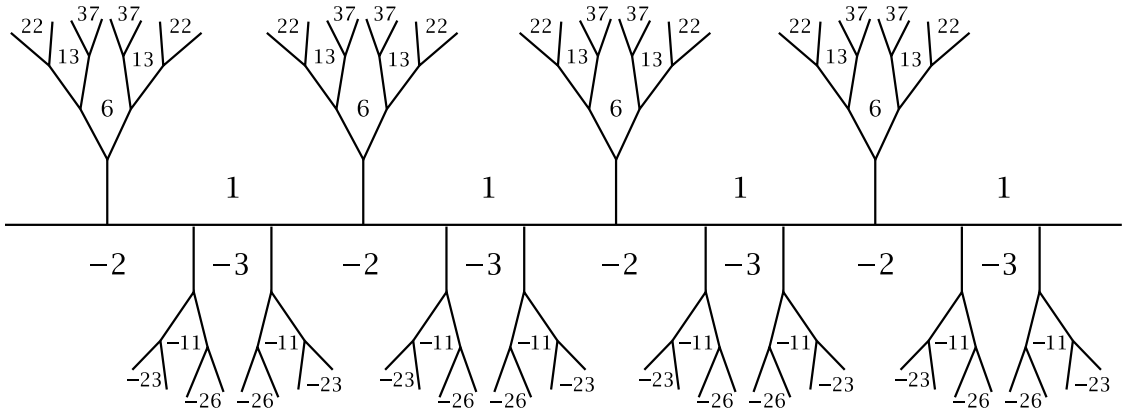
To extend the separator line one step farther to the right, apply the arithmetic progression rule to compute the next value 2 using the arithmetic progression $-2, 1-1, 2$. Since this value 2 is positive, we place it above the horizontal line and insert a vertical edge to separate this 2 from the 1 to the left of it, as in (b) of the figure. Now we repeat the process with the next arithmetic progression $1, 2-1, 1$ and put the new 1 above the horizontal line with a vertical edge separating it from the previous 2, as shown in (c). At the next step we compute the next value -2 and place it below the horizontal line since it is negative, giving (d). One more step produces (e) where we see that further repetitions will produce a pattern that repeats periodically as we move to the right. The arithmetic progression rule also implies that it repeats periodically to the left, so it is periodic in both directions:



Thus we have the periodic separator line. To get the rest of the topograph we can then work our way upward and downward from the separator line, as shown in the original figure. As one moves upward from the separator line, the values of Q become larger and larger, approaching $+\infty$ monotonically, and as one moves downward the values approach $-\infty$ monotonically. The reason for this will become clear in the next chapter when we discuss something called the Monotonicity Property.

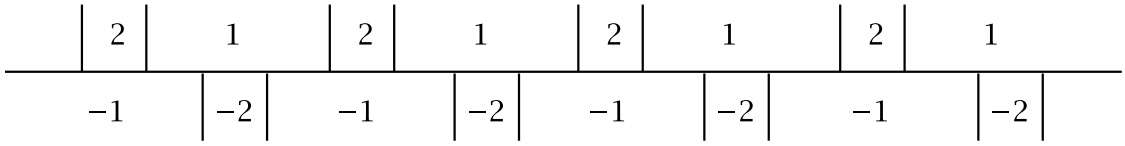
An interesting property of this form $x^2 - 2y^2$ that is evident from its topograph is that it takes on the same negative values as positive values. This would have been hard to predict from the formula $x^2 - 2y^2$. Indeed, for the similar-looking quadratic form $x^2 - 3y^2$ the negative values are quite different from the positive values, as one can see in its straightened-out topograph:

$Q(x, y) = x^2 - 3y^2$

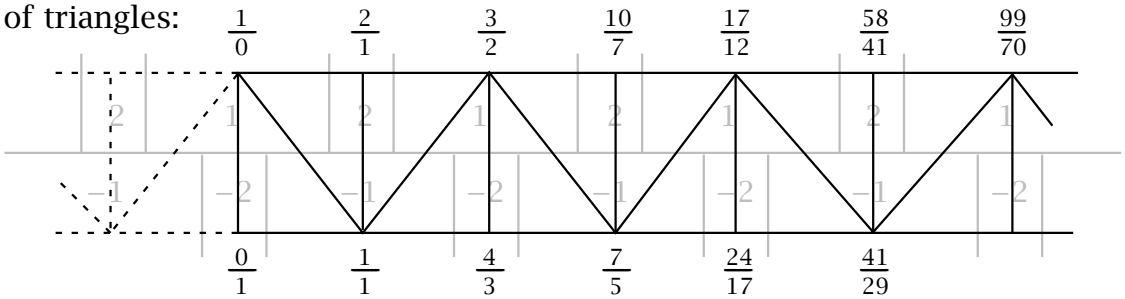


Continued Fractions Once More

There is a close connection between the topograph for a quadratic form $x^2 - dy^2$ and the infinite continued fraction for $\sqrt{d}$ when d is a positive integer that is not a square. In fact, we will see that the topograph can be used to compute the continued fraction for $\sqrt{d}$. As an example let us look at the case $d = 2$. The relevant portion of the topograph for $x^2 - 2y^2$ is the strip along the line separating the positive and negative values:



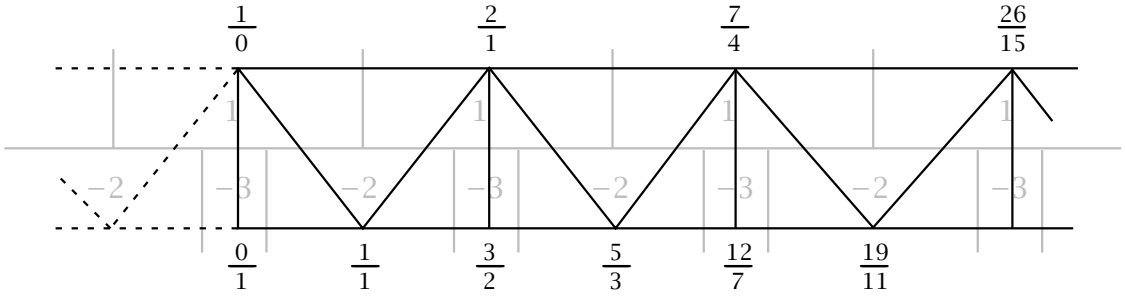
This is a part of the dual tree of the Farey diagram. If we superimpose the triangles of the Farey diagram corresponding to this part of the dual tree we obtain an infinite strip of triangles:



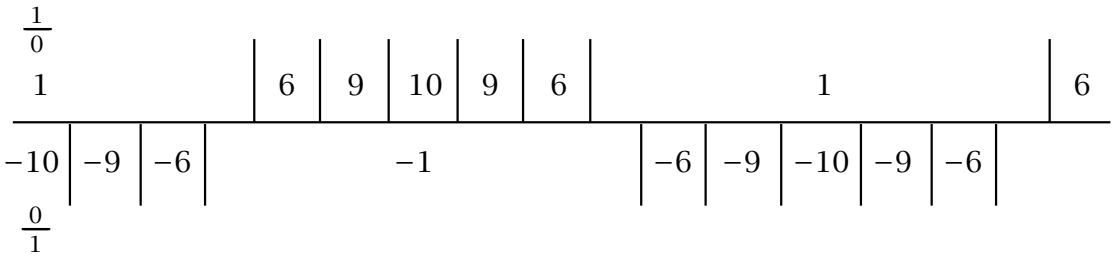
Ignoring the dotted triangles to the left, the infinite strip of triangles corresponds to the infinite continued fraction $1 + \overline{1/2}$. We could compute the value of this continued fraction by the method in Chapter 2, but there is an easier way using the quadratic

form $x^2 - 2y^2$. For fractions $\frac{x}{y}$ labeling the vertices along the infinite strip, the corresponding values $n = x^2 - 2y^2$ are either ± 1 or ± 2. We can rewrite the equation $x^2 - 2y^2 = n$ as $(\frac{x}{y})^2 = 2 + \frac{n}{y^2}$. As we go farther and farther to the right in the infinite strip, both x and y are getting larger and larger while n only varies through finitely many values, namely ± 1 and ± 2, so the quantity $\frac{n}{y^2}$ is approaching 0. The equation $(\frac{x}{y})^2 = 2 + \frac{n}{y^2}$ then implies that $(\frac{x}{y})^2$ is approaching 2, so we see that $\frac{x}{y}$ is approaching $\sqrt{2}$. Since the fractions $\frac{x}{y}$ are also approaching the value of the infinite continued fraction $1 + \overline{1/2}$ that corresponds to the infinite strip, this implies that the value of the continued fraction $1 + \overline{1/2}$ is $\sqrt{2}$.

Here is another example, for the quadratic form $x^2 - 3y^2$, showing how $\sqrt{3} = 1 + \overline{1/1 + 1/2}$.

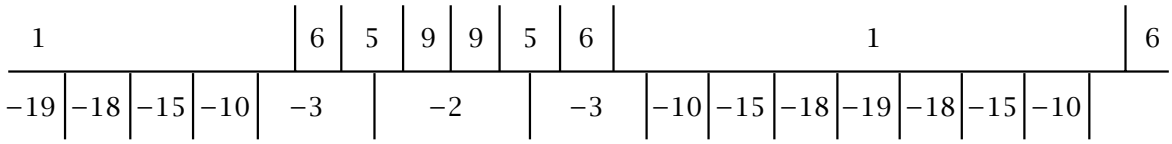


After looking at these two examples one can see that it is not really necessary to draw the strip of triangles, and one can just read off the continued fraction directly from the periodic separator line. Let us illustrate this by considering the form $x^2 - 10y^2$:



If one moves toward the right along the horizontal line starting at a point in the edge separating the $\frac{1}{0}$ region from the $\frac{0}{1}$ region, one first encounters 3 edges leading off to the right (downward), then 6 edges leading off to the left (upward), then 6 edges leading off to the right, and so on. This means that the continued fraction for $\sqrt{10}$ is $3 + \overline{1/6}$.

Here is a more complicated example showing how to compute the continued fraction for $\sqrt{19}$:

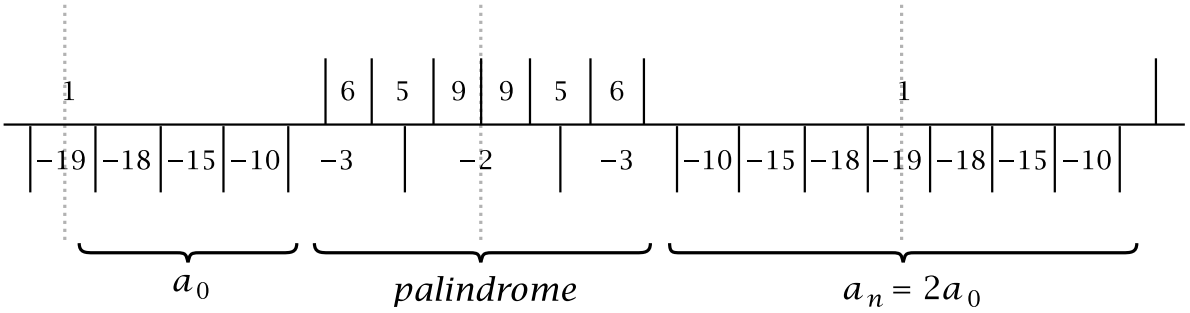


From this we read off that $\sqrt{19} = 4 + \overline{1/2 + 1/1 + 1/3 + 1/1 + 1/2 + 1/8}$.

In the next chapter we will prove that the topograph of the form $x^2 - dy^2$ always has a periodic separator line whenever d is a positive integer that is not a square. As in the examples above, this separator line always includes the edge of the dual tree separating the vertices $1/0$ and $0/1$ since the form takes the positive value $+1$ on $1/0$ and the negative value $-d$ on $0/1$. The periodicity then implies that the continued fraction for $\sqrt{d}$ has the form

$$\sqrt{d} = a_0 + \overline{1/a_1 + 1/a_2 + \cdots + 1/a_n}$$

with the periodic part starting immediately after the initial term a_0. In addition to being periodic, the separator line also has mirror symmetry with respect to reflection across the vertical line corresponding to the edge connecting $1/0$ to $0/1$ in the Farey diagram. This is because the form $x^2 - dy^2$ has no xy term, so replacing x/y by $-x/y$ does not change the value of the form. Once the separator line has symmetry with respect to this vertical line, the periodicity forces it to have mirror symmetry with respect to an infinite sequence of vertical lines, as illustrated in the following figure for the form $x^2 - 19y^2$:



In particular, these mirror symmetries imply that the continued fraction

$$\sqrt{d} = a_0 + \overline{1/a_1 + 1/a_2 + \cdots + 1/a_n}$$

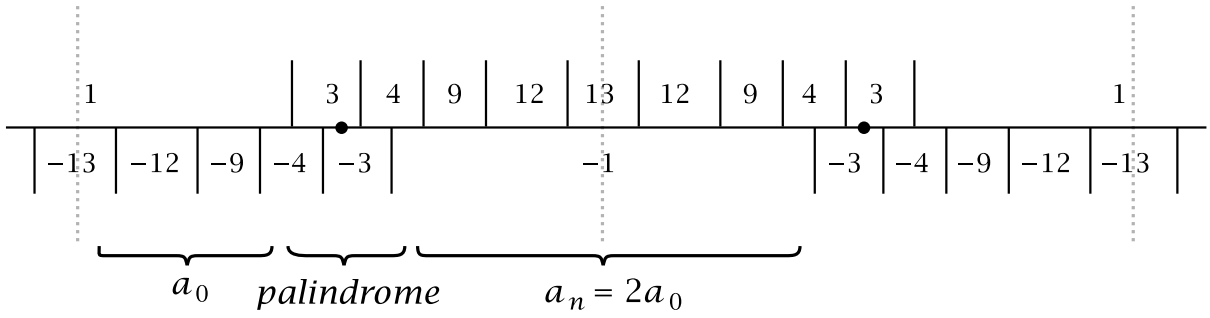
always has two special properties:

(a) $a_n = 2a_0$.

(b) The intermediate terms $a_1, a_2, \cdots, a_{n-1}$ form a palindrome, reading the same forward as backward.

Thus in $\sqrt{19} = 4 + \overline{1/2 + 1/1 + 1/3 + 1/1 + 1/2 + 1/8}$ the final 8 is twice the initial 4, and the intermediate terms $2, 1, 3, 1, 2$ form a palindrome. These special properties held also in the earlier examples, but were less apparent because there were fewer terms in the repeated part of the continued fraction.

In some cases there is an additional kind of symmetry along the separator line, as illustrated for the form $x^2 - 13y^2$:



As before there is a horizontal translation giving the periodicity and there are reflectional symmetries across vertical lines, but now there is an extra glide-reflection along the strip that interchanges the positive and negative values of the form. Performing this glide-reflection twice in succession gives the translational periodicity. Notice that there are also 180 degree rotational symmetries about the points marked with dots on the separator line, and these rotations account for the palindromic middle part of the continued fraction

$$\sqrt{13} = 3 + \overline{1/1 + 1/1 + 1/1 + 1/1 + 1/6}$$

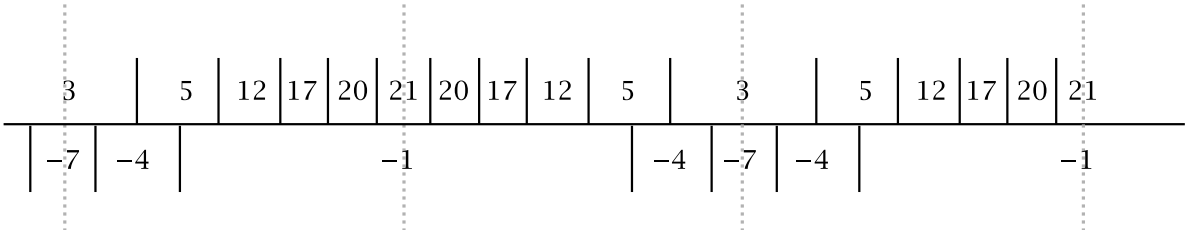
The fact that the periodic part has odd length corresponds to the separator strip having the glide-reflection symmetry. We could rewrite the continued fraction to have a periodic part of even length by doubling the period,

$$\sqrt{13} = 3 + \overline{1/1 + 1/1 + 1/1 + 1/1 + 1/6 + 1/1 + 1/1 + 1/1 + 1/1 + 1/6}$$

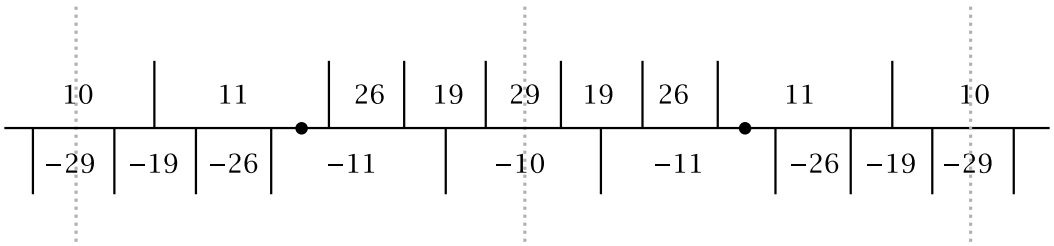
and this corresponds to ignoring the glide-reflection and just considering the translational periodicity.

We have been using quadratic forms $x^2 - dy^2$ to compute the continued fractions for irrational numbers $\sqrt{d}$, but everything works just the same for irrational numbers $\sqrt{p/q}$ if one uses the quadratic form $qx^2 - py^2$ in place of $x^2 - dy^2$. Following the same reasoning as before, if the equation $qx^2 - py^2 = n$ is rewritten as $q(\frac{x}{y})^2 = p + \frac{n}{y^2}$ then we see that as we move out along the periodic separator line the numbers x and y approach infinity while n cycles through finitely many values, so the term $\frac{n}{y^2}$ approaches 0 and the fractions $\frac{x}{y}$ approach a number z satisfying $qz^2 = p$, so $z = \sqrt{p/q}$. This argument depends of course on the existence of a periodic separator line, and we will prove in the next chapter that forms $qx^2 - py^2$ always have a periodic separator line, assuming that $\sqrt{p/q}$ is not a rational number, i.e., that p and q are not both squares.

Here are two examples. For the first one we use the form $3x^2 - 7y^2$ to compute the continued fraction for $\sqrt{7/3}$.



This gives $\sqrt{7/3} = 1 + \overline{1/1 + 1/1 + 1/8 + 1/1 + 1/1 + 1/2}$. For the second example we use $10x^2 - 29y^2$ to compute the continued fraction for $\sqrt{29/10}$,



with the result that $\sqrt{29/10} = 1 + \overline{1/1 + 1/2 + 1/2 + 1/1 + 1/2}$. The period of odd length here corresponds to the existence of the glide-reflection and 180 degree rotation symmetries.

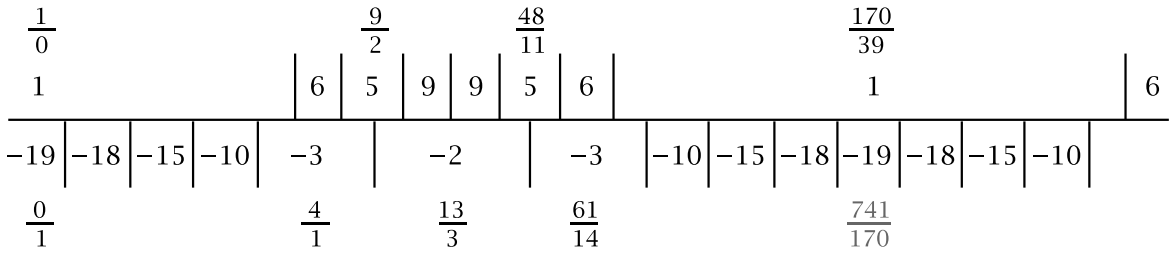
As one can see in these examples, the palindrome property and the relation $a_n = 2a_0$ still hold for the continued fractions for irrational numbers $\sqrt{p/q}$ assuming that $a_0 > 0$, which is equivalent to the condition $p/q > 1$ since a_0 is the integer part of $\sqrt{p/q}$. Fractions p/q less than 1 can easily be dealt with just by inverting them, interchanging p and q. Inverting a continued fraction $a_0 + \overline{1/a_1 + 1/a_2 + \cdots + 1/a_n}$ changes it to $1/a_0 + \overline{1/a_1 + 1/a_2 + \cdots + 1/a_n}$. For example, from the earlier computation of $\sqrt{7/3}$ we obtain $\sqrt{3/7} = 1/1 + \overline{1/1 + 1/1 + 1/8 + 1/1 + 1/1 + 1/2}$.

One might ask whether the irrational numbers $\sqrt{p/q}$ are the only numbers having a continued fraction $a_0 + \overline{1/a_1 + 1/a_2 + \cdots + 1/a_n}$ or $1/a_0 + \overline{1/a_1 + 1/a_2 + \cdots + 1/a_n}$ satisfying the palindrome property and the relation $a_n = 2a_0$. The answer is yes [and it would not be hard to prove this using the methods we are developing in this book].

Pell's Equation

We encountered the equation $x^2 - dy^2 = 1$ briefly in Chapter 0. It is traditionally called Pell's equation, and the similar equation $x^2 - dy^2 = -1$ is sometimes called Pell's equation as well, or the negative Pell's equation. If d is a square then the equations are not very interesting since in this case d can be incorporated into the y^2 term, so one is looking at the equations $x^2 - y^2 = 1$ and $x^2 - y^2 = -1$, which have only the trivial solutions $(x, y) = (\pm 1, 0)$ for the first equation and $(x, y) = (0, \pm 1)$ for the second equation, since these are the only cases when the difference between two squares is ± 1. We will therefore assume that d is not a square in what follows.

As an example let us look at the equation $x^2 - 19y^2 = 1$. We drew a portion of the periodic separator line for the form $x^2 - 19y^2$ earlier, and here it is again with some of the fractional labels x/y shown as well.



Ignoring the label $741/170$ for the moment, the other fractional labels are the first few convergents for the continued fraction for $\sqrt{19}$ that we computed before, $4 + \overline{1/2 + 1/1 + 1/3 + 1/1 + 1/2 + 1/8}$. These fractional labels are the labels on the vertices of the zigzag path in the infinite strip of triangles in the Farey diagram, which we can imagine being superimposed on the separator line in the figure. The fractional label we are most interested in is the $170/39$ because this is the label on a region where the value of the form $x^2 - 19y^2$ is 1. This means exactly that $(x, y) = (170, 39)$ is a solution of $x^2 - 19y^2 = 1$. In terms of continued fractions, the fraction $170/39$ is the value of the initial portion $4 + 1/2 + 1/1 + 1/3 + 1/1 + 1/2$ of the continued fraction for $\sqrt{19}$, with the final term of the period omitted.

Since the topograph of $x^2 - 19y^2$ is periodic along the separator line, there are infinitely many different solutions of $x^2 - 19y^2 = 1$ along the separator line. Going toward the left just gives the negatives $-x/y$ of the fractions x/y to the right, changing the signs of x or y, so it suffices to see what happens toward the right. One way to do this is to use the linear fractional transformation that gives the periodicity translation toward the right. This transformation sends the edge $\langle 1/0, 0/1\rangle$ of the Farey diagram to the edge $\langle 170/39, 741/170\rangle$. Here $741/170$ is the value of the continued fraction $4 + 1/2 + 1/1 + 1/3 + 1/1 + 1/2 + 1/4$ obtained from the continued fraction for $\sqrt{19}$ by replacing the final number 8 in the period by one-half of its value, 4. The figure above shows why this is the right thing to do. We get an infinite sequence of larger and larger positive solutions of $x^2 - 19y^2 = 1$ by applying the periodicity transformation with matrix $\left(\begin{smallmatrix} 170 & 741 \\ 39 & 170 \end{smallmatrix}\right)$ to the vector $(1, 0)$. For example,

$$\begin{pmatrix} 170 & 741 \\ 39 & 170 \end{pmatrix} \begin{pmatrix} 170 \\ 39 \end{pmatrix} = \begin{pmatrix} 57799 \\ 13260 \end{pmatrix}$$

so the next solution of $x^2 - 19y^2 = 1$ after $(170, 39)$ is $(57799, 13260)$, and we could compute more solutions if we wanted. Obviously they are getting large rather quickly.

The two 170's in the matrix $\left(\begin{smallmatrix} 170 & 741 \\ 39 & 170 \end{smallmatrix}\right)$ can hardly be just a coincidence. Notice also that the entry 741 factors as $19 \cdot 39$ which hardly seems like it should be just a coincidence either. Let's check that these numbers had to occur. In general, for the form $x^2 - dy^2$ let us suppose that we have found the first solution $(x, y) = (p, q)$ after $(1, 0)$ for Pell's equation $x^2 - dy^2 = 1$, so $p^2 - dq^2 = 1$. Then based on the previous example we suspect that the periodicity transformation is the transformation

$$\begin{pmatrix} p & dq \\ q & p \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} px + dqy \\ qx + py \end{pmatrix}$$

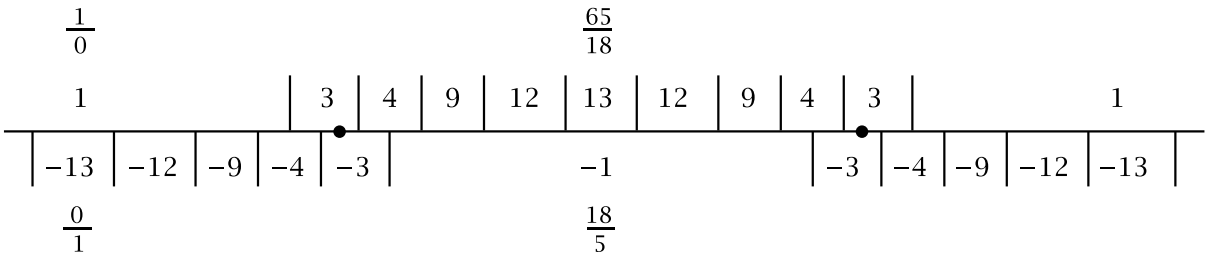
To check that this is correct the main thing to verify is that this transformation preserves the values of the quadratic form. When we plug in $(px + dqy, qx + dy)$ for (x, y) in $x^2 - dy^2$ we get

$$\begin{aligned}(px + dqy)^2 - d(qx + py)^2 \\ &= p^2x^2 + 2pdqxy + d^2q^2y^2 - dq^2x^2 - 2pdqxy - dp^2y^2 \\ &= (p^2 - dq^2)x^2 - d(p^2 - dq^2)y^2 \\ &= x^2 - dy^2 \quad \text{since } p^2 - dq^2 = 1\end{aligned}$$

so the transformation $\left(\begin{smallmatrix} p & dq \\ q & p \end{smallmatrix}\right)$ does preserve the values of the form. Also it takes $1/0$ to p/q, and its determinant is $p^2 - dq^2 = 1$, so it has to be the translation giving the periodicity along the separator line. (We haven't actually proved yet that periodic separator lines always exist for forms $x^2 - dy^2$, but we will do this in the next chapter.)

Are there other solutions of $x^2 - 19y^2 = 1$ besides the ones we have just described that occur along the separator line? The answer is No because we will see in the next chapter that as one moves away from the separator line in the topograph, the values of the quadratic form change in a monotonic fashion, steadily increasing toward $+\infty$ as one moves upward above the separator line, and decreasing steadily toward $-\infty$ as one moves downward below the separator line. Thus the value 1 occurs only along the separator line itself. Also we see that the value -1 never occurs, which means that the equation $x^2 - 19y^2 = -1$ has no integer solutions.

For an example where $x^2 - dy^2 = -1$ does have solutions, let us look again at the earlier example of $x^2 - 13y^2$.



The first positive solution $(x, y) = (p, q)$ of $x^2 - 13y^2 = -1$ corresponds to the value -1 in the middle of the figure. This is determined by the continued fraction $p/q = 3 + 1/(1 + 1/(1 + 1/(1 + 1/1))) = 18/5$, so we have $(p, q) = (18, 5)$. The matrix $\left(\begin{smallmatrix} p & dq \\ q & p \end{smallmatrix}\right)$ in this case is $\left(\begin{smallmatrix} 18 & 65 \\ 5 & 18 \end{smallmatrix}\right)$ with determinant $18^2 - 13 \cdot 5^2 = -1$ so this gives the glide-reflection along the periodic separator line taking $1/0$ to $18/5$ and $0/1$ to $65/18$. The smallest positive solution of $x^2 - 13y^2 = +1$ is obtained by applying this glide-reflection to $(18, 5)$, which gives

$$\begin{pmatrix} 18 & 65 \\ 5 & 18 \end{pmatrix} \begin{pmatrix} 18 \\ 5 \end{pmatrix} = \begin{pmatrix} 324 + 325 \\ 90 + 90 \end{pmatrix} = \begin{pmatrix} 649 \\ 180 \end{pmatrix}$$

Repeated applications of the glide-reflection will give solutions of $x^2 - 13y^2 = +1$ and $x^2 - 13y^2 = -1$ alternately.

Exercises

1. Draw the topograph for the form $Q(x,y) = 2x^2 + 5y^2$, showing all the values of $Q(x,y) \le 60$ in the topograph, with the associated fractional labels x/y. If there is symmetry in the topograph, you only need to draw one half of the topograph and state that the other half is symmetric.

2. Do the same for the form $Q(x,y) = 2x^2 + xy + 2y^2$, in this case displaying all values $Q(x,y) \le 40$ in the topograph.

3. Do the same for the form $Q(x,y) = x^2 - y^2$, showing all the values between $+30$ and -30 in the topograph, but omitting the labels x/y this time.

4. For the form $Q(x,y) = 2x^2 - xy + 3y^2$ do the following:
(a) Draw the topograph, showing all the values $Q(x,y) \le 30$ in the topograph, and including the labels x/y.
(b) List all the values $Q(x,y) \le 30$ in order, including the values when the pair (x,y) is not primitive.
(c) Find all the integer solutions of $Q(x,y) = 24$, both primitive and nonprimitive. (And don't forget that quadratic forms always satisfy $Q(x,y) = Q(-x,-y)$.)

5. Determine the periodic separator line in the topograph for each of the following quadratic forms (you do not need to include the fractional labels x/y):
(a) $x^2 - 7y^2$ (b) $3x^2 - 4y^2$ (c) $x^2 + xy - y^2$

6. Using your answers in the preceding problem, write down the continued fraction expansions for $\sqrt{7}$, $2\sqrt{3}/3$, and $(-1+\sqrt{5})/2$.

7. For the following quadratic forms, draw enough of the topograph, starting with the edge separating the $1/0$ and $0/1$ regions, to locate the periodic separator line, and include the separator line itself in your topograph.
(a) $x^2 + 3xy + y^2$ (b) $6x^2 + 18xy + 13y^2$ (c) $37x^2 - 104xy + 73y^2$

8. Use a quadratic form to compute continued fractions for the following pairs of numbers:
(a) $(3+\sqrt{6})/2$ and $(3-\sqrt{6})/2$ (b) $(11+\sqrt{13})/6$ and $(11-\sqrt{13})/6$
(c) $(14+\sqrt{7})/9$ and $(14-\sqrt{7})/9$

9. For the quadratic form $x^2 - 14y^2$ do the following things:
(a) Draw the separator line in the topograph and compute the continued fraction for $\sqrt{14}$.
(b) Find the smallest positive integer solutions of $x^2 - 14y^2 = 1$ and $x^2 - 14y^2 = -1$, if these equations have integer solutions.
(c) Find the linear fractional transformation that gives the periodicity translation along the separator line and use this to find a second positive solution of $x^2 - 14y^2 = 1$.
(d) Determine the integers n with $|n| \le 12$ such that the equation $x^2 - 14y^2 = n$ has

an integer solution. (Don't forget the possibility that there could be solutions (x, y) that aren't primitive.)

10. For the quadratic form $x^2 - 29y^2$ do the following things:
(a) Draw the separator line and compute the continued fraction for $\sqrt{29}$.
(b) Find the smallest positive integer solution of $x^2 - 29y^2 = -1$.
(c) Find a glide-reflection symmetry of the separator line and use this to find the smallest positive integer solution of $x^2 - 29y^2 = 1$.

11. Compute the periodic separator line for the form $x^2 - 43y^2$ and use this to find the continued fraction for $\sqrt{43}$.

Chapter 5. The Classification of Quadratic Forms

We can divide quadratic forms $Q(x,y) = ax^2+bxy+cy^2$ into four broad classes according to the signs of the values $Q(x,y)$ for $(x,y) \neq (0,0)$, where as always we restrict x and y to integers. (We assume at least one of the coefficients a,b,c is nonzero, so Q is not identically zero.)

(I) $Q(x,y)$ takes on both positive and negative values but not 0. In this case we call Q a *hyperbolic* form.

(II) $Q(x,y)$ takes on both positive and negative values and also 0. Then we call Q a 0*-hyperbolic* form.

(III) $Q(x,y)$ takes on only positive values or only negative values. Then we call Q *elliptic*.

(IV) Q takes on the value 0 and either positive or negative values, but not both. Then Q is called *parabolic*.

The hyperbolic-elliptic-parabolic terminology is motivated in part by what the level curves $ax^2 + bxy + cy^2 = k$ are, where we now allow x and y to take on all real values so that one gets actual curves. The level curves are hyperbolas in cases (I) and (II), and ellipses in case (III). In case (IV), however, the level curves are not parabolas as one might guess, but straight lines. Case (IV) will be the least interesting of the four cases.

There is an easy way to distinguish the four cases by looking at the discriminant $\Delta = b^2 - 4ac$:

(I) If Δ is positive but not a square then Q is hyperbolic.

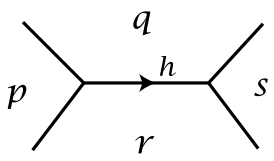
(II) If Δ is positive and a square then Q is 0-hyperbolic.

(III) If Δ is negative then Q is elliptic.

(IV) If Δ is zero then Q is parabolic.

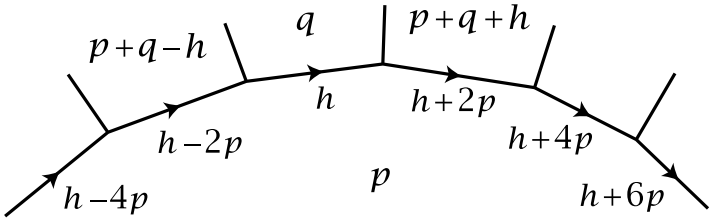
These statements will be proved later in this chapter.

We will analyze each of the four types of forms in turn, but before doing this let us make a couple preliminary general comments. In the arithmetic progression rule for labeling the four regions surrounding a given edge of the topograph, we can label the edge by the common increment $h = (q+r) - p = s - (q+r)$ as in the figure at the right. The edge can be oriented by an arrow showing the direction in which the progression increases by h. Changing the sign of h corresponds to changing the orientation of the edge. In the special case that h happens to be 0 the orientation of the edge is irrelevant and can be omitted.



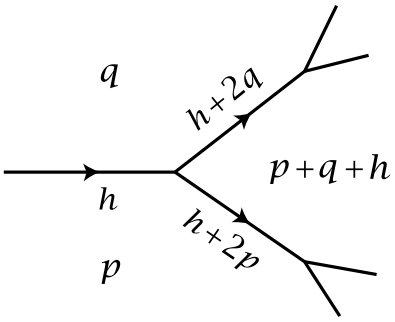
The values of the increment h along the boundary of a region in the topograph have the interesting property that they also form an arithmetic progression, when all these edges are oriented in the same direction, and the amount by which h increases

as we move from one edge to the next is $2p$ where p is the label on the region adjacent to all these edges:



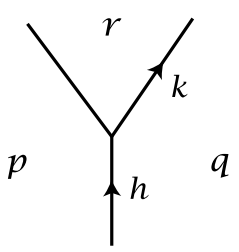
We will call this property the *Second Arithmetic Progression Rule*. To see why it is true, start with the edge labeled h in the figure, with the adjacent regions labeled p and q. The original Arithmetic Progression Rule then gives the value $p+q+h$ in the next region to the right. From this we can deduce that the label on the edge between the regions labeled p and $p+q+h$ must be $h+2p$ since this is the increment from q to $p+(p+q+h)$. Thus the edge label increases by $2p$ when we move from one edge to the next edge to the right, so by repeated applications of this fact we see that we have an arithmetic progression of edge labels all along the border of the region labeled p.

Another thing worth noting at this point is something that we will refer to as the *Monotonicity Property*: If the three labels p, q, and h adjacent to an edge are all positive, then so are the three labels for the next two edges in front of this edge (orienting these edges as shown in the figure), and the new labels are larger than the old labels. It follows that when one continues forward out this part of the topograph, all the labels become monotonically larger the farther one goes. Similarly, when the original three labels are negative, all the labels become larger and larger negative, by the same principle applied to the negative $-Q(x,y)$ of the original form $Q(x,y)$.



Proposition. *If an edge in the topograph of $Q(x,y)$ is labeled h with adjacent regions labeled p and q, then the quantity h^2-4pq is equal to the discriminant of $Q(x,y)$.*

Proof: For the given form $Q(x,y)=ax^2+bxy+cy^2$, the regions $1/0$ and $0/1$ in the topograph are labeled a and c, and the edge in the topograph separating these two regions has $h=b$ since the $1/1$ region is labeled $a+b+c$. So the statement of the proposition is correct for this edge. For other edges we proceed by induction, moving farther and farther out the tree. For the induction step suppose we have two adjacent edges labeled h and k as in the figure, and suppose inductively that the discriminant equals h^2-4pq. We have $r=p+q+h$, and from the second arithmetic progression rule we know that $k=h+2q$. Then we have $k^2-4qr=(h+2q)^2-4q(p+q+h)=h^2+4hq+4q^2-4pq-4q^2-4hq=h^2-4pq$,



which means that the result holds for the edge labeled k as well. □

Hyperbolic Forms

The most interesting of the four types of quadratic forms are the hyperbolic forms. We will show that these all have a periodic separator line as in the examples $x^2 - dy^2$ and $qx^2 - py^2$ that we looked at earlier.

Theorem. *For a hyperbolic form $Q(x, y)$ the edges of the topograph for which the two adjacent regions are labeled by numbers of opposite sign form a line which is infinite in both directions, and the topograph is periodic along this line.*

Proof: Since the form is hyperbolic, all regions of the topograph have labels that are either positive or negative, never zero. There must exist two regions of opposite sign since Q is hyperbolic, and by moving along a path in the topograph joining these two regions we will somewhere encounter two adjacent regions of opposite sign. Thus there must exist edges whose two adjacent regions have opposite sign. Let us call these edges *separating edges*. If we apply the discriminant formula $\Delta = h^2 - 4pq$ in preceding proposition to a separating edge, we see that Δ must be positive since p and q are nonzero and have opposite sign, so $-4pq$ is positive while h^2 is positive or zero. Thus a hyperbolic form must have positive discriminant.

At an end of a separating edge the value of Q in the next region must be either positive or negative since Q does not take the value 0:

This implies that exactly one of the two edges at the end of the first separating edge is also a separating edge. Repeating this argument, we see that each separating edge is part of a line of separating edges that is infinite in both directions (and the edges that lead off from this edge are not separating edges).

As we move off this line of separating edges the values of Q are steadily increasing on the positive side and steadily decreasing on the negative side, by the monotonicity property, so there are no other separating edges that are not on this line.

It remains to prove that the topograph is periodic along the separator line. We can assume all the edges along the line are oriented in the same direction, by changing the signs of the h values where necessary. For an edge of the line labeled h with adjacent regions labeled p and $-q$, with $p, q > 0$, we know that $h^2 + 4pq$ is equal to the discriminant Δ. From the equation $\Delta = h^2 + 4pq$ we obtain the inequalities $|h| < \sqrt{\Delta}$, $p \le \Delta/4$, and $q \le \Delta/4$. Thus there are only finitely many possible values for h, p, and q along the separator line. Hence there are only finitely many possible combinations of values h, p, and q at each edge on the separator line. It follows that

there must be two edges on the line that have the same values of h, p, and q. Since the topograph is uniquely determined by the three labels h, p, q at a single edge, the translation of the line along itself that takes one edge to another edge with the same three labels must preserve all the labels on the line. This shows that the separator line is periodic, including the values of Q. □

Conceivably there might be just a single region on one side of the separator line, but this doesn't actually happen. There must be edges leading away from the separating line on both the side where the form is positive and on the side where it is negative. For if there was just a single region on one side of the line, the second arithmetic progression rule would say that the h labels along the line formed an infinite arithmetic progression, contradicting the fact that these values are periodic.

Here is an interesting consequence of the periodicity of the separator line:

Corollary. *For a hyperbolic form $Q(x,y) = ax^2 + bxy + cy^2$, if the equation $ax^2 + bxy + cy^2 = n$ has one integer solution then it has infinitely many integer solutions.*

Proof: Suppose (x,y) is a solution of $Q(x,y) = n$. If (x,y) is a primitive pair, then the number n appears in the topograph of Q infinitely many times, via the periodicity of the separator line, so there are infinitely many solutions in this case. If (x,y) is not primitive then it is m times a primitive pair (x',y') with $Q(x',y') = n/m^2$. This latter equation has infinitely many solutions as we just saw, so after replacing these solutions (x',y') by $(x,y) = (mx',my')$ we get infinitely many solutions of $Q(x,y) = n$. □

In Chapter 3 we gave an argument that showed that infinite continued fractions that are eventually periodic always represent quadratic irrational numbers. This is one half of Lagrange's Theorem, and now we can prove the other half, the converse statement:

Theorem. *The continued fraction expansion of every quadratic irrational is eventually periodic.*

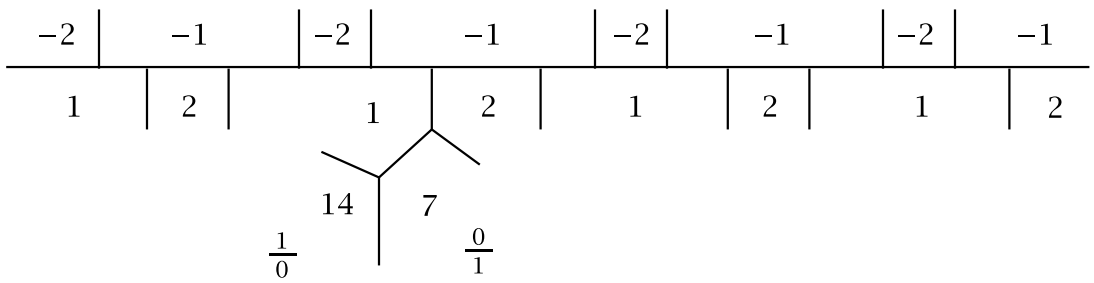
Proof: A quadratic irrational number α has the form $A + B\sqrt{n}$ where A and B are rational numbers and n is a positive integer that is not a square. Letting $\overline{\alpha}$ be the conjugate $A - B\sqrt{n}$ of α, we see that α and $\overline{\alpha}$ are roots of the quadratic equation $(x-\alpha)(x-\overline{\alpha}) = x^2 - 2Ax + (A^2 - nB^2) = 0$ whose coefficients are rational numbers. After multiplying through by a common denominator we can replace this equation by an equation $ax^2 + bx + c = 0$ with integer coefficients having α and $\overline{\alpha}$ as roots. The leading coefficient a is nonzero since it arose from multiplying by a common denominator.

From the quadratic equation $ax^2 + bx + c = 0$ we obtain a quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ with the same coefficients a,b,c. We claim that this

quadratic form is hyperbolic. It cannot take on the value 0 at an integer pair $(x,y) \neq (0,0)$ since if $ax^2+bxy+cy^2=0$ then we cannot have $y=0$, otherwise the equation would become $ax^2=0$ with $a\neq 0$, forcing x to be 0 as well. Since $y\neq 0$ we can divide the equation $ax^2+bxy+cy^2=0$ by y^2 to get a quadratic equation $a(x/y)^2+b(x/y)+c=0$ with a rational root x/y, contrary to the assumption that the root α, and hence also $\overline{\alpha}$, was irrational. Thus the quadratic form $Q(x,y)$ does not take on the value 0. To see that $Q(x,y)$ takes on both positive and negative values, note that $a(x/y)^2+b(x/y)+c$ takes on both positive and negative values at rational numbers x/y since the graph of the function ax^2+bx+c is a parabola crossing the x-axis at two distinct points α and $\overline{\alpha}$. Multiplying the formula $a(x/y)^2+b(x/y)+c$ by the positive number y^2, it follows that $ax^2+bxy+cy^2$ also takes on both positive and negative values at integer pairs (x,y).

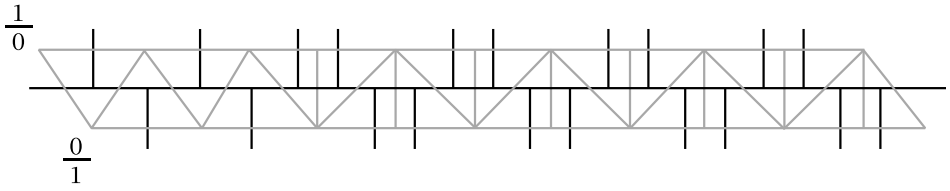
Since Q is hyperbolic, its topograph contains a periodic line separating the positive and negative values. This corresponds to a strip in the Farey diagram which is infinite in both directions. The fractions x_n/y_n labeling the vertices along this strip have both x_n and y_n approaching $\pm\infty$ as n goes to $\pm\infty$. (The only way this could fail for a path consisting of an infinite sequence of distinct edges in the dual tree would be if all the edges from some point onward bordered the $1/0$ or $0/1$ region, which is not the case here since periodic separator lines have only a finite number of edges bordering a given region.) The values $Q(x_n,y_n)=ax_n^2+bx_ny_n+cy_n^2=k_n$ are bounded, ranging over a finite set along the strip. Thus $a(x_n/y_n)^2+b(x_n/y_n)+c=k_n/y_n^2\to 0$ as $n\to\pm\infty$, so at one end of the strip we have $x_n/y_n\to\alpha$ and at the other end we have $x_n/y_n\to\overline{\alpha}$. Joining either end of the strip to $1/0$ in the Farey diagram then gives infinite strips corresponding to infinite continued fractions for α and $\overline{\alpha}$ that are eventually periodic. □

Let us look at an example to illustrate the procedure in the proof of this theorem. We will use a quadratic form to compute the continued fractions for the two quadratic irrationals $\frac{10\pm\sqrt{2}}{14}$. The equation $(x-\alpha)(x-\overline{\alpha})=0$ is $x^2-\frac{10}{7}x+\frac{1}{2}=0$, so with integer coefficients this becomes $14x^2-20x+7=0$. The associated quadratic form is $14x^2-20xy+7y^2$. To compute the topograph we start with the three values at $1/0$, $0/1$, and $1/1$ and work toward the separator line:



This figure lies in the upper half of the circular Farey diagram where the fractions x/y are positive, so if we follow the separator line out to the right we approach the

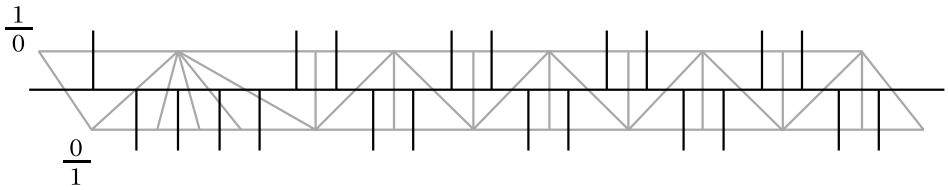
smaller of the two roots of $14x^2 - 20x + 7 = 0$, which is $\frac{10-\sqrt{2}}{14}$, and if we follow the separator line to the left we approach the larger root, $\frac{10+\sqrt{2}}{14}$. To get the continued fraction for the smaller root we follow the path in the figure that starts with the edge between $1/0$ and $0/1$, then zigzags up to the separator line, then goes out this line to the right. If we straighten this path out it looks like the following:



The continued fraction is therefore

$$\frac{10-\sqrt{2}}{14} = 1/1 + 1/1 + 1/1 + 1/1 + \overline{1/2}$$

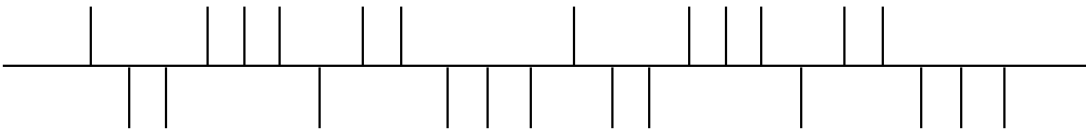
It is not actually necessary to redraw the straightened-out path since in the original form of the topograph we can read off the sequence of left and right "side roads" as we go along the path, the sequence $LRLR\overline{LLRR}$ where L denotes a side road to the left and R a side road to the right. This sequence determines the continued fraction. For the other root $\frac{10+\sqrt{2}}{14}$ the straightened-out path has the following shape:



The sequence of side roads is $LRRRR\overline{LLRR}$ so the continued fraction is

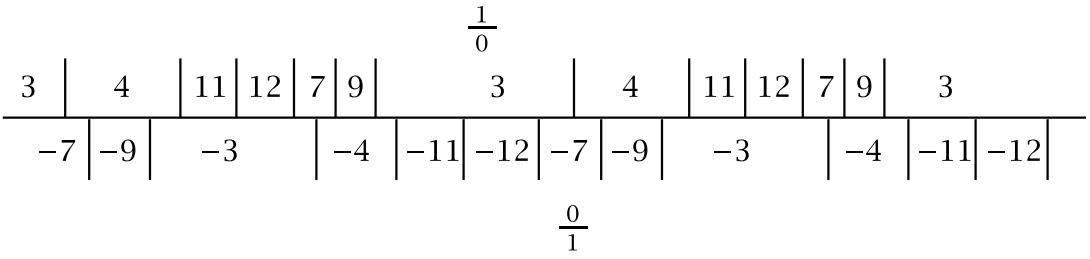
$$\frac{10+\sqrt{2}}{14} = 1/1 + 1/4 + \overline{1/2}$$

A natural question to ask is whether every periodic line in the dual tree of the Farey diagram is the separator line of some hyperbolic form, and the answer is yes. To find the form one first uses the periodic line to construct a continued fraction that is eventually periodic, then one computes the value of this continued fraction by finding a quadratic equation that it satisfies, and this quadratic equation gives the desired quadratic form. As an example, let us find a quadratic form whose periodic line looks like the following:



A periodic continued fraction corresponding to this strip is $\overline{1/1 + 1/2 + 1/3}$. The value of this continued fraction was worked out in an example in Chapter 3 by finding a quadratic equation that it satisfies, which was $3x^2 + 8x - 7 = 0$ with roots $(-4 \pm$

$\sqrt{37})/3$. The positive root $(-4+\sqrt{37})/3$ is the value of $\overline{1/1+1/2+1/3}$. The corresponding quadratic form is $3x^2+8xy-7y^2$, and if we compute its separator line we get

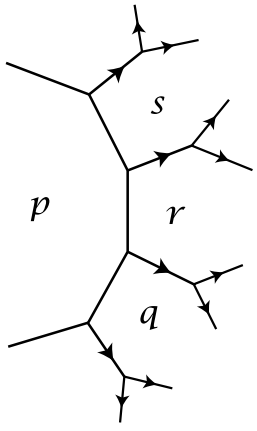


This provides a realization of the given periodic line as the separator line in the topograph of a quadratic form. Notice that the separator line is not symmetric under reflection across any vertical line, unlike all the separator lines we have seen up to this point. This is the simplest example without this bilateral symmetry property since the strips associated to continued fractions $\overline{1/a_1}$ and $\overline{1/a_1+1/a_2}$ obviously have bilateral symmetry, as do the strips for continued fractions $\overline{1/a_1+1/a_2+1/a_3}$ if two of the numbers a_1, a_2, a_3 are equal.

Elliptic Forms

An elliptic quadratic form $Q(x,y)$ takes on either all positive or all negative values at integer pairs $(x,y)\neq(0,0)$. The two cases are equivalent since one can switch from one to the other just by putting a minus sign in front of Q. Thus it suffices to consider the case that Q takes on only positive values, and we will assume we are in this case from now on. We will also generally assume when we look at topographs of elliptic forms that the orientations of the edges are chosen so as to give positive h-values, unless we state otherwise.

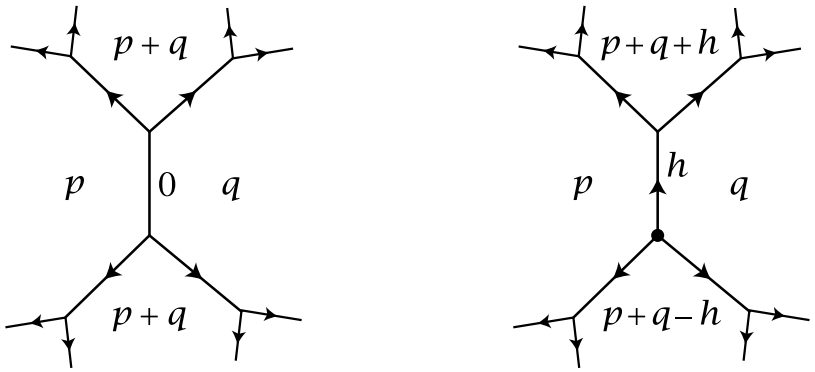
Let p be the minimum value taken on by Q, and consider a region of the topograph where Q takes the value p. All the edges having one endpoint at this region are oriented away from the region, by the arithmetic progression rule and the assumption that p is the minimum value of Q. The monotonicity property then implies that all edges farther away from the p region are also oriented away from the region, and the values of Q increase as one moves away from the region.



For the edges making up the border of the p region we know that the h-labels on these edges form an arithmetic progression with increment $2p$, provided that we temporarily reorient these edges so that they all point in the same direction. There are two possibilities for this arithmetic progression:

(I) Some edge bordering the p region has the label $h=0$. The topograph then has the form shown in the first figure below, with the orientations on edges that give positive

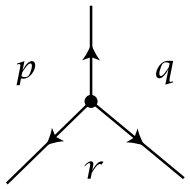
h-labels. An example of such a form is px^2+qy^2. We call the 0-labeled edge a *source edge* since all other edges are oriented away from this edge.



(II) No edge bordering the p region has label $h = 0$. Since the labels on these edges form an arithmetic progression, there must be some vertex where the terms in the progression change sign. Then when we orient the edges to give positive h-labels, all three edges meeting at this vertex will be oriented away from the vertex, as in the second figure above. We call this a *source vertex* since all edges in the topograph are oriented away from this vertex.

The fact that the three edges leading from a source vertex all point away from the vertex is equivalent to the three triangle inequalities

$$p < q + r \qquad q < p + r \qquad r < p + q$$



In the case of a source edge one of these inequalities becomes an equality $r = p + q$.

Proposition. *Elliptic forms have negative discriminant.*

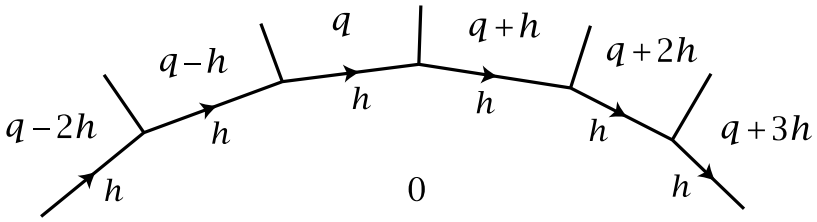
Proof: In the case of a source edge with the label $h = 0$ separating regions labeled p and q, the discriminant is $\Delta = h^2 - 4pq = -4pq$, which is negative. In the case of a source vertex with adjacent regions labeled p, q, r, the edge between the p and q regions is labeled $h = p + q - r$ so we have

$$\begin{aligned}\Delta = h^2 - 4pq &= (p + q - r)^2 - 4pq \\ &= p^2 + q^2 + r^2 - 2pq - 2pr - 2qr \\ &= p(p - q - r) + q(q - p - r) + r(r - p - q)\end{aligned}$$

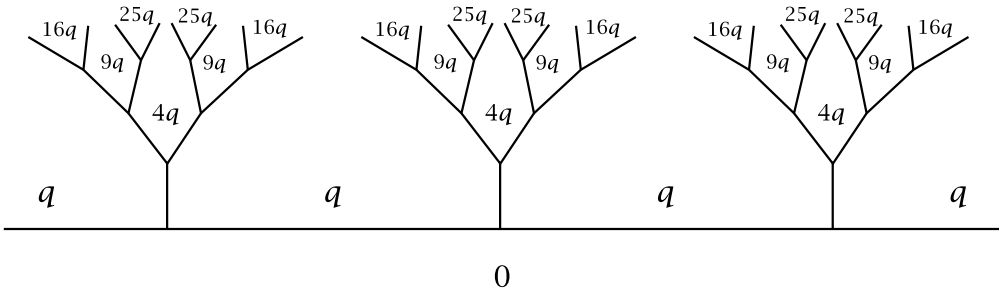
In the last line the three quantities in parentheses are negative by the triangle inequalities, so Δ is negative. □

Parabolic and 0-Hyperbolic Forms

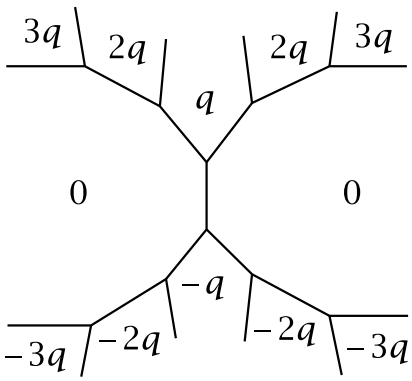
These are the forms whose topograph has at least one region labeled 0. Each edge adjacent to the 0 region has the same label h, and the labels on the regions adjacent to the 0 region form an arithmetic progression. The discriminant is $\Delta = h^2$, a square.



A special case is $h = 0$. Then the topograph is as shown in the next figure, and the form is parabolic with discriminant $\Delta = h^2 = 0$. Notice that the topograph is periodic along the 0 region since it consists of the same tree pattern repeated infinitely often.

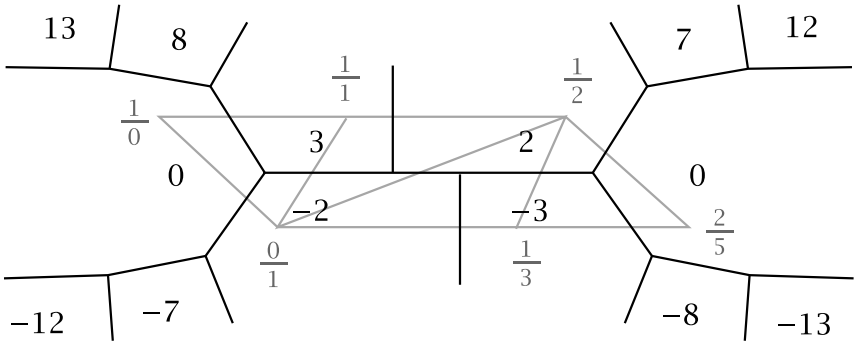


The remaining case is that h is nonzero, so the discriminant $\Delta = h^2$ is a nonzero square. The arithmetic progression of values of Q adjacent to the 0 region is not constant, so it includes both positive and negative numbers, and hence Q is 0-hyperbolic. If the arithmetic progression includes the value 0, this gives a second 0 region adjacent to the first one, and the topograph is as shown at the right. This is the topograph of the form $Q(x, y) = qxy$, with the two 0 regions at $x/y = 1/0$ and $0/1$.



If the arithmetic progression of values of Q adjacent to the 0 region does not include 0, there will be an edge separating the positive from the negative values in the progression. We can extend this separating edge to a line of separating edges as we did with hyperbolic forms, but the extension will eventually have to terminate with a second 0 region, otherwise the reasoning we used in the hyperbolic case would yield two edges along this line having the same h and the same positive and negative labels on the two adjacent regions, which would force the line to be periodic and hence extend infinitely far in both directions, which is impossible since it began at a 0 region at one end. Thus the topograph contains a finite separator line connecting two 0 regions. An example of such a form is $Q(x, y) = qxy - py^2 = (qx - py)y$ which has the value

0 at $x/y = 1/0$ and p/q. Here we must have $|q| > 1$ for the two 0 regions to be nonadjacent. The separator line follows the strip of triangles in the Farey diagram corresponding to the continued fraction for p/q. For example, for $p/q = 2/5$ the topograph of the form $5xy - 2y^2 = (5x - 2y)y$ is the following:



This completes our description of what parabolic and 0-hyperbolic forms look like. As we have seen, the discriminants of these forms are squares. The converse is also true:

Proposition. *If the discriminant of a form $Q(x,y)$ is a square, then $Q(x,y) = 0$ for some pair of integers $(x,y) \neq (0,0)$ so Q is either parabolic or 0-hyperbolic.*

Proof: Suppose first that the form $Q(x,y) = ax^2 + bxy + cy^2$ happens to have $a = 0$. Then $Q(1,0) = 0$ so we are done in this case (and note that $\Delta = b^2$, a square). So we can assume that $a \neq 0$. The equation $aX^2 + bX + c = 0$ then has roots $X = (-b \pm \sqrt{b^2 - 4ac})/2a$. If $b^2 - 4ac$ is a square, this means the roots are rational. If $X = p/q$ is a rational root then $a(p/q)^2 + b(p/q) + c = 0$ and hence $ap^2 + bpq + cq^2 = 0$ so Q takes the value 0 at a pair (p,q) with $q \neq 0$. □

In particular, this shows the discriminant of a hyperbolic form is not a square. Since we showed earlier that a hyperbolic form has positive discriminant, this completes the characterization of the four types of forms in terms of their discriminants.

Equivalence of Forms

In the pictures of topographs we have drawn, we often omit the fractional labels x/y for the regions in the topograph since the more important information is often just the values $Q(x,y)$ of the form. This leads to the idea of considering two quadratic forms to be equivalent if their topographs "look the same" when the labels x/y are disregarded. For a precise definition, one can say that quadratic forms Q_1 and Q_2 are equivalent if there is a vertex v_1 in the topograph of Q_1 and a vertex v_2 in the topograph of Q_2 such that the values of Q_1 in the three regions surrounding v_1 are equal to the values of Q_2 in the three regions surrounding v_2. Since the three values around a vertex determine all the other values in a topograph, this guarantees that the topographs look the same everywhere, if the labels x/y are omitted.

With this definition, a topograph and its mirror image correspond to equivalent forms since the mirror image topograph has the same three labels around each vertex as in the corresponding vertex of the original topograph. For example, switching the variables x and y reflects the circular Farey diagram across its vertical axis and hence reflects the topograph of a form $Q(x,y)$ to the topograph of the equivalent form $Q(y,x)$. As another example, the forms $ax^2+bxy+cy^2$ and $ax^2-bxy+cy^2$ are equivalent since they are related by changing (x,y) to $(-x,y)$, reflecting the Farey diagram across its horizontal axis, with a corresponding reflection of the topograph.

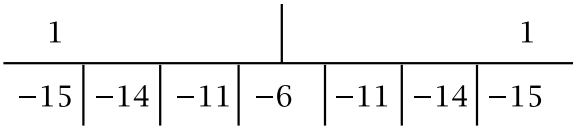
Theorem. *Up to equivalence, there are just a finite number of forms with a given discriminant, except in the special case that the discriminant is zero.*

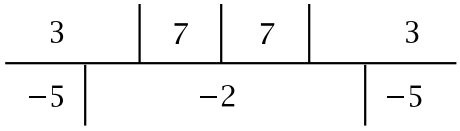
This fails to hold for forms of discriminant 0, the parabolic forms, since multiplying such a form by different integers produces infinitely many inequivalent forms.

Proof: Consider first the case of forms of positive discriminant. These are either hyperbolic or 0-hyperbolic. Hyperbolic forms have a separator line. For an edge in the separator line labeled h with adjacent regions labeled $p>0$ and $-q<0$ we have $\Delta = h^2+4pq$, so each of the quantities $|h|$, p, and q is bounded in size by Δ. This means that for fixed Δ there are only finitely many possibilities for h, p, and q for each edge of the separator line, hence just finitely many possible combinations of h, p, and $-q$ for each edge, so there are just finitely many possibilities for the form, up to equivalence. The same reasoning applies also to 0-hyperbolic forms that have a separating edge in their topograph. The only ones that do not have a separating edge are the ones with two adjacent regions labeled 0. In this case the edge separating these two regions has $h^2=\Delta$, so the value of h on this edge is determined by Δ, hence the form is determined by Δ.

For forms of negative discriminant we can assume we are dealing with positive elliptic forms since a form Q and its negative $-Q$ have the same discriminant. If a positive elliptic form has a source edge in its topograph, this edge has $h=0$ so $\Delta=-4pq$ where p and q are the values of Q in the adjacent regions. For fixed Δ there are only finitely many choices of p and q satisfying $\Delta=-4pq$, so there are only finitely many positive elliptic forms of discriminant Δ having a source edge. In the other case of a source vertex surrounded by values p,q,r of the form, we obtained the formula $\Delta = p(p-q-r)+q(q-p-r)+r(r-p-q)$ with the three quantities in parentheses being negative, so $p+q+r\le|\Delta|$ and hence there are only finitely many possibilities for p, q, and r for each Δ. □

As an example, let us determine all the quadratic forms of discriminant 60, up to equivalence. Two obvious forms of discriminant 60 are x^2-15y^2 and $3x^2-5y^2$, whose separator lines consist of periodic repetitions of the following two patterns:



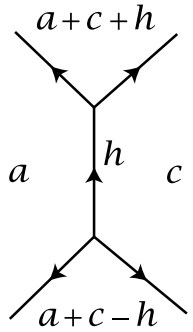


From these topographs it is apparent that the two forms are not equivalent, and also that the negatives of these two forms, $-x^2 + 15y^2$ and $-3x^2 + 5y^2$, give two more inequivalent forms, for a total of four equivalence classes. To see whether there are others we use the formula $\Delta = 60 = h^2 + 4pq$ relating the values p and $-q$ along an edge labeled h in the separator line, with $p > 0$ and $q > 0$. The various possibilities are listed in the table below. Note that the equation $60 = h^2 + 4pq$ implies that h has to be even. (In fact, the general formula $\Delta = h^2 - 4ac$ implies that h and Δ always have the same parity.)

h	pq	(p,q)
0	15	$(1,15),\ (3,5),\ (5,3),\ (15,1)$
2	14	$(1,14),\ (2,7),\ (7,2),\ (14,1)$
4	11	$(1,11),\ (11,1)$
6	6	$(1,6),\ (2,3),\ (3,2),\ (6,1)$

Each pair of values for (p,q) in the table occurs at some edge along the separator line in one of the two topographs shown above, or the negatives of these topographs. Hence every form of discriminant 60 is equivalent to one of these four. If it had not been true that all the possibilities in the table occurred in the topographs of the forms we started with, we could have used these other possibilities for h, p, and q to generate new topographs and hence new forms, eventually exhausting all the finitely many possibilities.

For finding all the positive elliptic quadratic forms of a given discriminant, up to equivalence, the procedure is simpler since it is not actually necessary to draw any topographs. At a source vertex or edge in the topograph for such a form Q let the smaller two of the three adjacent values of Q be $a \le c$, with the edge between them labeled $h \ge 0$, so that the third adjacent value of Q is $a + c - h$. The form is then equivalent to the form $ax^2 + hxy + cy^2$. Since a and c are the smallest values of Q we have $a \le c \le a + c - h$, and the latter inequality implies that $h \le a$. Thus we have the inequalities $0 \le h \le a \le c$. Note that these inequalities imply the three triangle inequalities at the source vertex or edge: $a + c - h \le a + c$, $a < c + (a + c - h)$, and $c < a + (a + c - h)$. For the discriminant $\Delta = -D$ we have $D = 4ac - h^2$, so we are seeking solutions of



$$4ac = h^2 + D \qquad \text{with} \quad 0 \le h \le a \le c$$

The number h must have the same parity as D, and we can bound the choices for h by the inequalities $4h^2 \le 4a^2 \le 4ac = D + h^2$ which imply $3h^2 \le D$, or $h^2 \le D/3$. Every

positive elliptic form is equivalent to one of the forms $ax^2 + hxy + cy^2$ for triples (a,h,c) satisfying these conditions $4ac = h^2 + D$, $0 \le h \le a \le c$, and $h^2 \le D/3$. Different choices of (a,h,c) satisfying these conditions never give forms that are equivalent since a and c are the labels on the two regions in the topograph where the form takes its smallest values, and h is determined by a, c, and D by the formula $4ac = h^2 + D$.

As an example, when $D = 260$ we must have h even and $h^2 \le 260/3$ so h must be 0, 2, 4, 6, or 8. The corresponding values of a and c that are possible can then be computed from the equation $4ac = 260 + h^2$, always keeping in mind the requirement that $h \le a \le c$. The possibilities are shown in the following table:

h	ac	(a,c)
0	65	$(1,65)$, $(5,13)$
2	66	$(2,33)$, $(3,22)$, $(6,11)$
4	69	—
6	74	—
8	81	$(9,9)$

Thus every positive elliptic form of discriminant -260 is equivalent to one of the forms x^2+65y^2, $5x^2+13y^2$, $2x^2+2xy+33y^2$, $3x^2+2xy+22y^2$, $6x^2+2xy+11y^2$, or $9x^2 + 8xy + 9y^2$, and no two of these are equivalent to each other, as explained earlier.

A natural question is whether every integer occurs as the discriminant of some form, and this question is easy to answer. For a form $ax^2 + bxy + cy^2$ we have $\Delta = b^2 - 4ac$, and this is congruent to b^2 mod 4. A square such as b^2 is always congruent to 0 or 1 mod 4, so the discriminant of a form is always congruent to 0 or 1 mod 4. Conversely, for every integer Δ congruent to 0 or 1 mod 4 there exists a form whose discriminant is Δ. Namely, if $\Delta = 4k$ then the form $x^2 - ky^2$ has discriminant $4k$, and if $\Delta = 4k + 1$ then the form $x^2 + xy - ky^2$ has discriminant $4k+1$. Here k can be positive, negative, or zero. The forms x^2-ky^2 and $x^2+xy-ky^2$ are called the *principal* quadratic forms of these discriminants.

Orientation-Preserving Equivalence

Our definition of equivalence of forms specifies that two forms are equivalent if the topograph of one can be transformed into the topograph of the other by some linear fractional transformation. This transformation can either preserve orientation or reverse it. We can obtain a more refined notion of equivalence by only allowing transformations that preserve orientation. Thus a topograph and its mirror image may no longer be equivalent under this more strict notion of equivalence. As an example, let us look at the earlier example of discriminant $\Delta = -260$ where we saw that there were six equivalence classes of forms. Small portions of the topographs of these six forms are shown below.

In the first two topographs the central edge is a source edge, and in the other four the lower vertex is a source vertex. Whenever there is a source edge the topograph has a mirror symmetry across a line perpendicular to the source edge. When there is source vertex there is a mirror symmetry only when at least two of the three surrounding values of the form are equal, as in the third and sixth topographs above, but not the fourth or fifth topographs. Thus the mirror images of the fourth and fifth topographs correspond to two more quadratic forms which are not equivalent to them under any orientation-preserving transformation. To obtain an explicit formula for the mirror image forms we can just interchange the a and c terms in $ax^2 + bxy + cy^2$, which in this case gives the new forms $22x^2 + 2xy + 3y^2$ and $11x^2 + 2xy + 6y^2$. The net result of all this is that with the more refined notion of equivalence there are eight equivalence classes.

The Class Number

The number of equivalence classes of quadratic forms with a given discriminant, where one only considers forms having positive values in the elliptic case, is known as the *class number* for the given discriminant. Of special interest are the cases when the class number is 1, so all forms of that discriminant are equivalent. There are nine negative discriminants $\Delta = -D$ of class number 1:

$$\Delta = -3,\ -4,\ -7,\ -8,\ -11,\ -19,\ -43,\ -67,\ -163$$

It was conjectured by Gauss around 1800 that this is the complete list for negative discriminants. It was shown in the 1930s that there is at most one more, and then in the 1960s the possibility of an elusive tenth such discriminant was finally ruled out, finishing the proof of the conjecture. For positive discriminant there are many more cases where the class number is 1, but it is still unknown whether there are infinitely many such discriminants. The available computational evidence seems to indicate that there are infinitely many.

In the nine cases $D = 3, 4, 7, 8, 11, 19, 43, 67, 163$ it is very easy to check that all forms are equivalent. For example when $D = 163$ we must have h odd with $h^2 \le 163/3$ so the only possibilities are $h = 1, 3, 5, 7$. From the equation $4ac = 163 + h^2$ the corresponding values of ac are $41, 43, 47, 53$ which all happen to be primes, and since $a \le c$ this forces a to be 1 in each case. But since $h \le a$ this means h must be 1, and we obtain the single quadratic form $ax^2 + hxy + cy^2 = x^2 + xy + 41y^2$.

The corresponding polynomial $x^2 + x + 41$ has a curious property discovered by Euler: For each $x = 0, 1, 2, \cdots, 39$ the value of $x^2 + x + 41$ is a prime number. Here are these primes:

41 43 47 53 61 71 83 97 113 131 151 173 197 223 251 281 313 347 383 421
461 503 547 593 641 691 743 797 853 911 971 1033 1097 1163 1231 1301
1373 1447 1523 1601

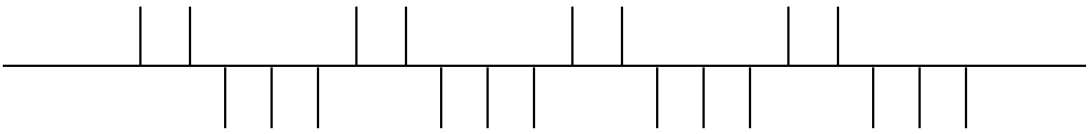
Notice that the successive differences between these numbers are $2, 4, 6, 8, \cdots$. The next number in the sequence would be $1681 = 41^2$, not a prime. (Write $x^2 + x + 41$ as $x(x+1) + 41$ to see why $x = 40$ must give a nonprime value.) A similar thing happens for the other values of D. The nontrivial cases are:

D		
7	$x^2 + x + 2$	2
11	$x^2 + x + 3$	3 5
19	$x^2 + x + 5$	5 7 11 17
43	$x^2 + x + 11$	11 13 17 23 31 41 53 67 83 101
67	$x^2 + x + 17$	17 19 23 29 37 47 59 73 89 107 127 149 173 199 227 257

It's interesting that these lists include all primes less than 100 except for 79.

Exercises

1. Find a hyperbolic quadratic form whose periodic separator line has the following pattern:



2. In this problem we consider only quadratic forms $Q(x, y) = ax^2 + cy^2$ with no xy term, for the sake of simplicity.
(a) Find two 0-hyperbolic forms $ax^2 + cy^2$ that have the same discriminant but take on different sets of values. Draw enough of the topographs of the two forms to make it apparent that they do not have exactly the same sets of values. (Remember that the topograph only shows the values $Q(x, y)$ for primitive pairs (x, y).)
(b) Do the same thing with two elliptic forms that take on positive values. Include the source vertex or source edge in the topographs.
(c) Do the same thing with two hyperbolic forms, drawing their separator lines.

3. (a) Show the quadratic form $Q(x, y) = 92x^2 - 74xy + 15y^2$ is elliptic by computing its discriminant.
(b) Find the source vertex or edge in the topograph of this form.
(c) Using the topograph of this form, find all the integer solutions of $92x^2 - 74xy + 15y^2 = 60$, and explain why your list of solutions is a complete list. (There are exactly four pairs of solutions $\pm(x, y)$, three of which will be visible in the topograph.)

4. (a) Show that if a quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ can be factored as a product $(Ax + By)(Cx + Dy)$ with A, B, C, D integers, then Q takes the value 0 at some pair of integers $(x, y) \neq (0, 0)$, hence Q must be either 0-hyperbolic or parabolic. Show also, by a direct calculation, that the discriminant of this form is a square.

(b) Find a 0-hyperbolic form $Q(x, y)$ such that $Q(1, 5) = 0$ and $Q(7, 2) = 0$ and draw a portion of the topograph of Q that includes the two regions where $Q = 0$.

5. Determine the number of equivalence classes of quadratic forms of discriminant $\Delta = 120$ and list one form from each equivalence class.

6. Do the same thing for $\Delta = 61$.

7. (a) Find the smallest positive nonsquare discriminant for which there is more than one equivalence class of forms of that discriminant. (In particular, show that all smaller discriminants have only one equivalence class.)
(b) Find the smallest positive nonsquare discriminant for which there are two inequivalent forms of that discriminant, neither of which is simply the negative of the other.

8. (a) For positive elliptic forms of discriminant $\Delta = -D$, verify that the smallest value of D for which there are at least two inequivalent forms of discriminant $-D$ is $D = 12$.
(b) If we add the requirement that neither of the two inequivalent forms is a constant multiple of some other form with smaller D, then what is the smallest D?

9. Determine all the equivalence classes of positive elliptic forms of discriminants -67, -104, and -347.

10. (a) Determine all the equivalence classes of 0-hyperbolic forms of discriminant 49.
(b) Determine which equivalence class in part (a) each of the forms $Q(x, y) = 7xy - py^2$ for $p = 0, 1, 2, 3, 4, 5, 6$ belongs to.

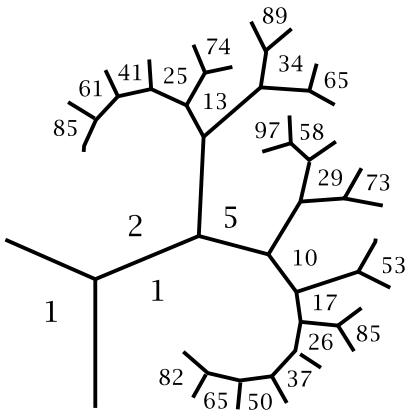
Chapter 6. Representations by Quadratic Forms

With the various things we have learned about quadratic forms so far, let us return to the basic problem of trying to determine what values a given form $Q(x,y)$ can take on, or in different terminology, determining which numbers are represented by Q. Remember that it suffices to restrict attention to the values in the topograph since these are the values for primitive pairs (x,y), and to get all possible values one just multiplies the values in the topograph by arbitrary squares. We focus on the forms that are either elliptic or hyperbolic, as these are the most interesting cases.

As we will see through a series of examples, the type of answer one gets to the representation problem varies from quite simple to slightly complicated to quite complicated indeed.

The First Level of Complexity

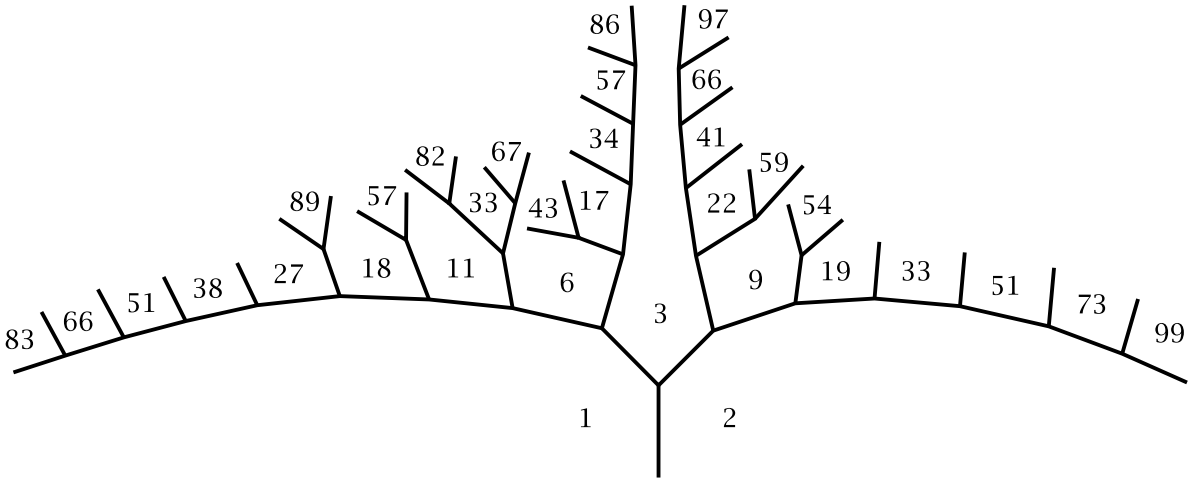
As a first example let us try to find a general pattern in the values of the form $x^2 + y^2$. In view of the symmetry of the topograph for this form it suffices to look just in the first quadrant of the topograph. A piece of this quadrant is shown in the figure at the right, somewhat distorted to squeeze more numbers into the picture. What is shown is all the numbers in the topograph that are less than 100. At first glance it seems hard to find any patterns here, but the key is to look at how the numbers in the topograph factor into primes. First of all, the primes that occur in the topograph are $2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97$. Apart from 2, these are just the primes congruent to 1 modulo 4. The remaining primes are congruent to 3 modulo 4, namely, $3, 7, 11, 19, 23, 31, 43, 47, 59, 71, 79, 83$, and these do not appear in the topograph. Moreover, all the numbers in the topograph that are not prime are products of primes in the topograph: $10, 25, 26, 34, 50, 58, 65, 74, 82, 85$. If we remember that the topograph only shows the values of $Q(x,y)$ for primitive pairs (x,y), this means that the remaining values of $Q(x,y)$ are obtained from those in the topograph by multiplying by an arbitrary square m^2. Thus we are led to predict that the following result might be true:



Theorem of Fermat. *The values of the quadratic form $Q(x,y) = x^2 + y^2$ as x and y range over all integers are exactly the numbers of the form $m^2 p_1 p_2 \cdots p_k$ where m is an arbitrary integer and each p_i is either 2 or a prime congruent to 1 modulo 4.*

Here we allow the possibility that the number of prime factors p_i in $m^2 p_1 p_2 \cdots p_k$ is zero, so the number represented by Q is simply m^2, which is $Q(m,0)$. We will prove this theorem later in this chapter.

As a second example consider the form $Q(x,y) = x^2 + 2y^2$. Here is a portion of its topograph showing all values less than 100 again:



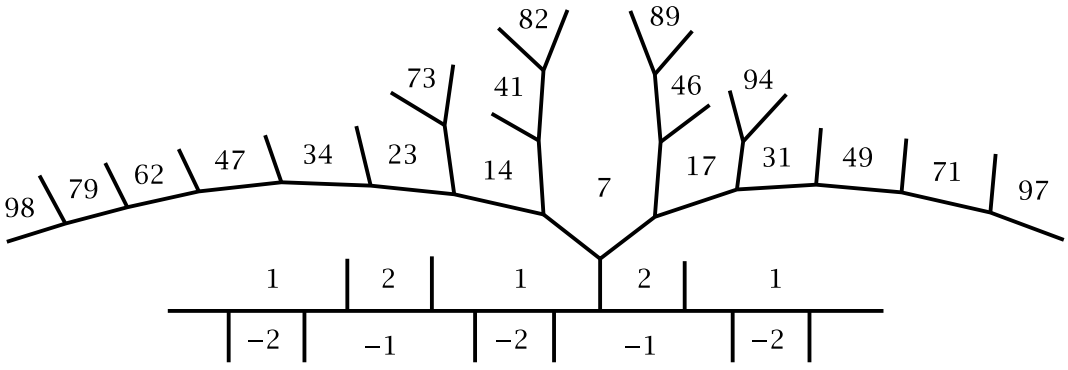
Inspecting the values here, we see that the following two statements appear to be true:

(1) The prime numbers that occur as values of $x^2 + 2y^2$ are 2 and the primes congruent to 1 or 3 modulo 8. In the part of the topograph shown these are $3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97$. The remaining primes are congruent to 5 or 7 modulo 8 and these do not occur as values of $x^2 + 2y^2$.

(2) The values of $x^2 + 2y^2$ are exactly the numbers that can be expressed as products $m^2 p_1 p_2 \cdots p_k$ where m is an arbitrary integer and each p_i is a prime values of $x^2 + 2y^2$ as in (1).

These statements are in fact true and were also known to Fermat.

These two examples were elliptic forms, but the same sort of behavior can occur for hyperbolic forms, as we see in the next example, the form $x^2 - 2y^2$. The negative values of this form happen to be just the negatives of the positive values, so we need only show the positive values in the topograph:



Here the primes that occur are 2 and primes congruent to 1 or 7 modulo 8. We can count the negative of a prime number as a prime as well, and then the primes represented are ± 2 and the primes congruent to ± 1 modulo 8. The nonprime values are the products of the primes represented and squares times these numbers.

In these three examples the crucial idea was to look at prime factorizations and at

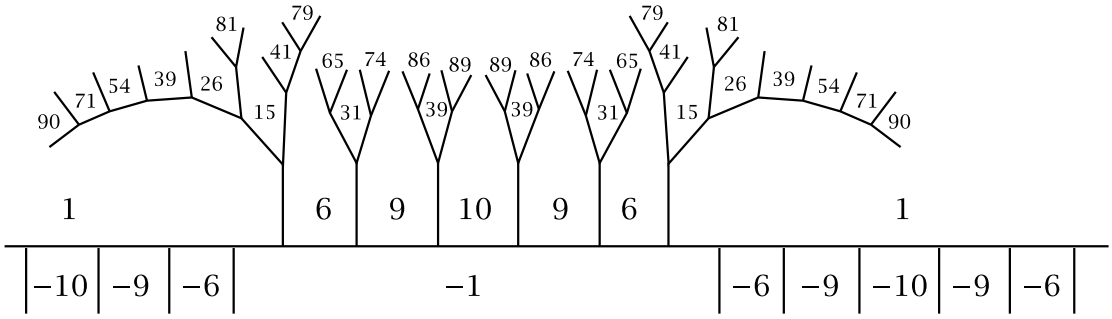
primes modulo certain numbers, the numbers 4, 8, and 8 in the three cases. Notice that these numbers are just the absolute values of the discriminants -4, -8, and 8 in the three cases. Looking at primes modulo $|\Delta|$ turns out to be a key idea for all quadratic forms, as we will see.

A special feature of the discriminants -4, -8, and 8 is that all forms of each of these discriminants are equivalent, or in other words, the class numbers are 1 for these discriminants. It is a general fact that whenever the class number is 1, the representation problem has the same sort of simple answer as in the examples above.

The Second Level of Complexity

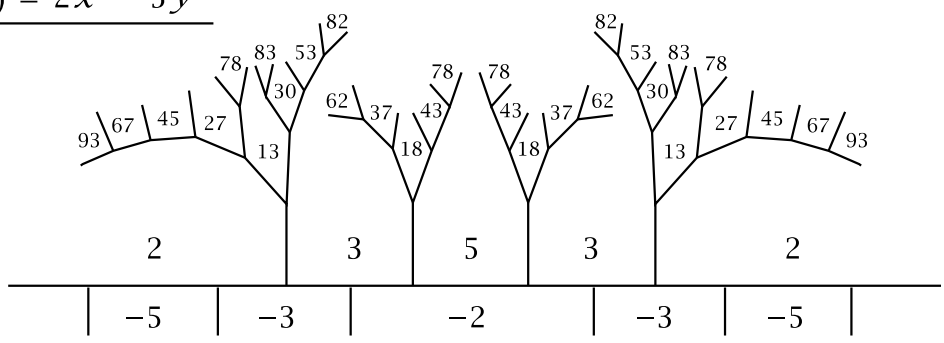
An example with slightly more complicated behavior is the form $x^2 - 10y^2$. Here is a portion of its topograph showing all the positive values less than 100:

$Q(x, y) = x^2 - 10y^2$



There is no need to show any more of the negative values since these will just be the negatives of the positive values. The prime values less than 100 are $31, 41, 71, 79, 89$. These are the primes congruent to ± 1 or ± 9 modulo 40, the discriminant. However, in contrast to what happened in the previous examples, there are many nonprime values that are not products of these prime values. In fact these nonprime values are products of the primes $2, 3, 5, 13, 37, 43$, none of which occur as a value of the form. Rather miraculously, these prime values are realized instead by another form $2x^2 - 5y^2$ having the same discriminant as $x^2 - 10y^2$. Here is the topograph of this companion form $2x^2 - 5y^2$:

$Q(x, y) = 2x^2 - 5y^2$



The prime values this form takes on are 2 and 5, which are the prime divisors of the discriminant 40, along with primes congruent to ± 3 and ± 13 modulo 40, namely

$3, 13, 37, 43, 53, 67, 83$.

Apart from the primes 2 and 5 that divide the discriminant 40, the possible values of primes modulo 40 are $\pm1, \pm3, \pm7, \pm9, \pm11, \pm13, \pm17, \pm19$ since even numbers and multiples of 5 are excluded. There are 16 different congruence classes here, and exactly half of them, 8, are realized by one or the other of the two forms $x^2 - 10y^2$ and $2x^2 - 5y^2$, with 4 classes realized by each form. The other 8 congruence classes are not realized by any form of discriminant 40 since every form of discriminant 40 is equivalent to one of the two forms $x^2 - 10y^2$ or $2x^2 - 5y^2$, as is easily checked by the methods from the previous chapter.

This is in fact a general phenomenon, valid for all discriminants: If one looks at primes that do not divide the discriminant, then the prime values of quadratic forms of that discriminant are exactly the primes in one-half of the possible congruence classes modulo the discriminant.

Let us mention in passing a famous theorem of Dirichlet, proved in the 1820s or 1830s, which says that every arithmetic progression $a, a+d, a+2d, a+3d, \cdots$ contains infinitely many primes, provided that one rules out the obvious exceptions where a and d have a common divisor, which would then be a common divisor of all the numbers in the progression. For example, when we take $d = 40$, each of the 16 congruence classes listed above gives an arithmetic progression containing infinitely many primes, such as the progression $1, 41, 81, 121, 161, 201, \cdots$ or the progression $17, 57, 97, 137, 177, 217, \cdots$. In fact Dirichlet proved more: If one looks at primes less than some large number N such as a million, then each of the possible congruence classes contains approximately the same number of primes less than N.

The analog of Fermat's Theorem for discriminant 40 is the following pair of statements:

(1) *The numbers represented by one of the two quadratic forms* $Q_1 = x^2 - 10y^2$ *or* $Q_2 = 2x^2 - 5y^2$ *of discriminant* 40 *are exactly the numbers* $n = \pm m^2 p_1 p_2 \cdots p_k$ *where* m *is an arbitrary integer and each* p_i *is* 2, 5, *or a prime congruent to* $\pm1, \pm3, \pm9$, *or* ±13 *modulo* 40.

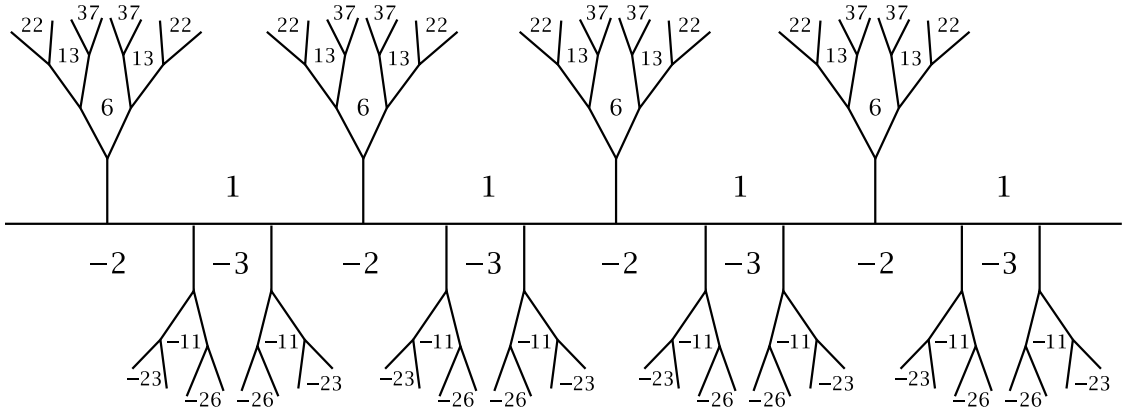
(2) *If the number of factors* p_i *in* $n = \pm m^2 p_1 p_2 \cdots p_k$ *that equal* 2, 5, *or* ±3 *or* ±13 *modulo* 40 *is even, then* n *is represented by* Q_1, *and if this number is odd then* n *is represented by* Q_2. *In particular, the primes represented by* Q_1 *are the primes congruent to* ±1 *or* ±9 *modulo* 40 *and the primes represented by* Q_2 *are* 2, 5, *and primes congruent to* ±3 *or* ±13 *modulo* 40.

An interesting consequence of (2) is that no number n is represented by both forms $x^2 - 10y^2$ and $2x^2 - 5y^2$, apart from $n = 0$ which is trivially represented by every form $Q(x, y)$ when $(x, y) = (0, 0)$.

Another case which is similar to the preceding one is discriminant 12. Here there are two forms up to equivalence, $x^2 - 3y^2$ and $3x^2 - y^2$, which is equivalent to

$-x^2+3y^2$, the negative of the first form. Here is the topograph for x^2-3y^2:

$Q(x,y) = x^2-3y^2$



For the form $-x^2+3y^2$ we get the negatives of the numbers represented by x^2-3y^2. For discriminant 12 we have the following answer to the representation problem:

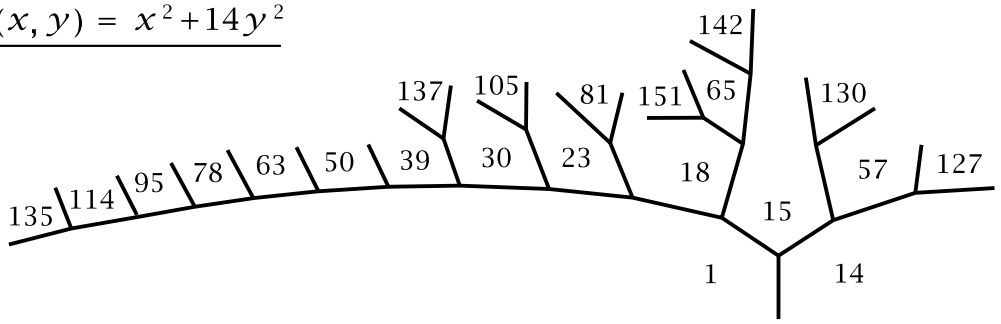
The numbers represented by one of the two quadratic forms x^2-3y^2 or $-x^2+3y^2$ of discriminant 12 are exactly the numbers $n = m^2p_1p_2\cdots p_k$ where m is an arbitrary integer and each p_i is -1, 2, 3, or a prime congruent to ±1 modulo 12. If the number of factors p_i equal to -1, 2, 3, or congruent to -1 modulo 12 is even, then n is represented by the form x^2-3y^2, and if this number is odd then n is represented by $-x^2+3y^2$.

The Third Level of Complexity

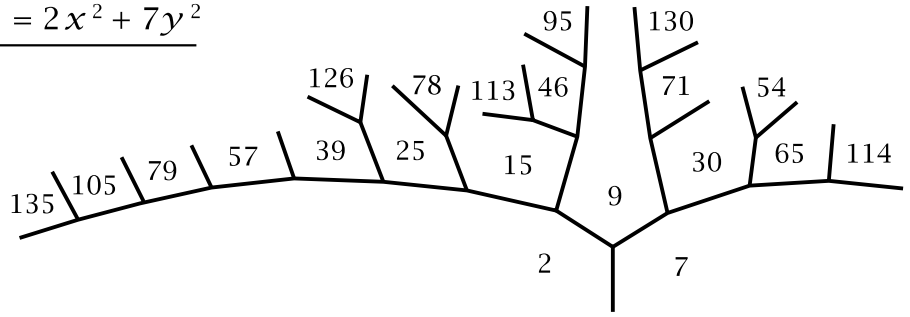
In the preceding examples it was possible to determine which numbers are represented by a given form by looking at primes and which congruence classes they fall into modulo the discriminant. A consequence of the way the answer was formulated was that no number (except 0) could by represented by two inequivalent forms of the same discriminant. Both of these nice properties fail to hold in general, however. An example is provided by forms of discriminant -56. Two inequivalent forms of this discriminant are $Q_1 = x^2+14y^2$ and $Q_2 = 2x^2+7y^2$. The primes 23 and 79 are congruent modulo 56, and yet 23 is represented by Q_1 since $Q_1(3,1) = 23$, while 79 is represented by Q_2 since $Q_2(6,1) = 79$. Also, 30 is represented by both Q_1 and Q_2 since $Q_1(4,1) = 30$ and $Q_2(1,2) = 30$.

The class number for discriminant -56 is actually 3, and a third form with this discriminant, not equivalent to either Q_1 or Q_2, is the form $Q_3 = 3x^2+2xy+5y^2$. Here are portions of the topographs of these three forms:

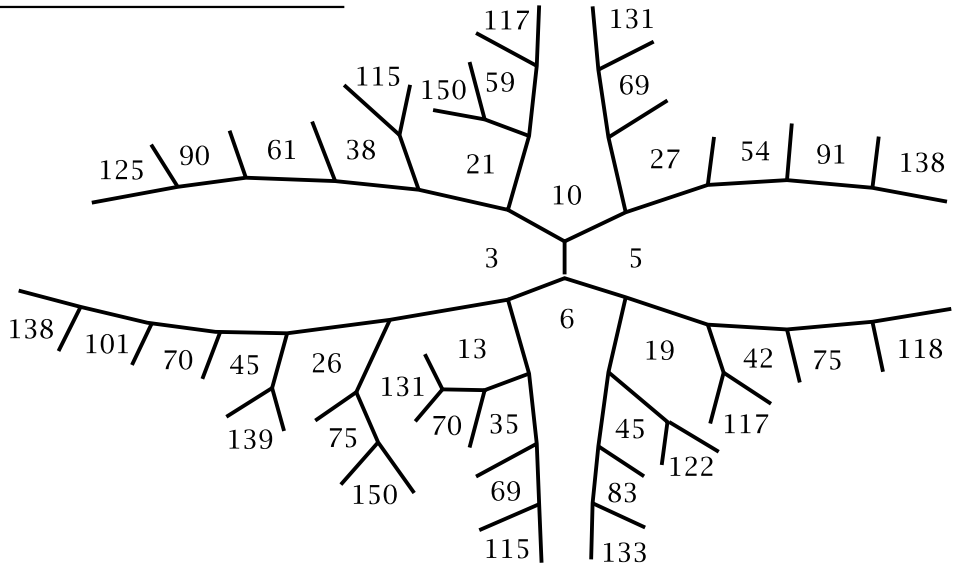
$Q_1(x,y) = x^2+14y^2$



$Q_2(x,y) = 2x^2+7y^2$



$Q_3(x,y) = 3x^2+2xy+5y^2$



Apart from the primes 2 and 7 that divide the discriminant -56, all other primes belong to the following 24 congruence classes modulo 56, corresponding to odd numbers less than 56 not divisible by 7:

$$\underline{1}\ \overline{3}\ \overline{5}\ \underline{9}\ 11\ \overline{13}\ \underline{15}\ 17\ \overline{19}\ \underline{23}\ \underline{25}\ \overline{27}\ 29\ 31\ 33\ 37\ \underline{39}\ 41\ 43\ \overline{45}\ 47\ 51\ 53\ 55$$

The six congruence classes whose prime elements are represented by Q_1 or Q_2 are indicated by underlines, and the six congruence classes whose prime elements are represented by Q_3 are indicated by overlines. Primes not represented by any of the three forms are in the remaining 12 congruence classes.

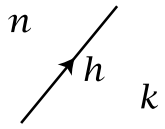
As general terminology, one says that two quadratic forms of the same discriminant belong to the same *genus* if they cannot be distinguished by considering their

values modulo the discriminant. Thus the preceding two forms Q_1 and Q_2 are of the same genus while Q_3 is of a different genus from Q_1 and Q_2. Equivalent forms always belong to the same genus, of course. The first two of the three levels of complexity we have described correspond to the discriminants where there is only one equivalence class in each genus. For discriminant -56 there are two different genera ("genera" is the plural of "genus"). In more complicated examples there can be large numbers of genera and large numbers of equivalence classes within a genus.

For negative discriminants there is a simple formula for the number of genera of forms of a given discriminant Δ, namely, the number of genera is 2^{k-1} where k is the number of distinct prime divisors of $|\Delta|$.

A Criterion for Representability

Suppose a number n is represented primitively by some form $Q(x,y)$ of discriminant Δ, so n appears in the topograph of Q. If we look at an edge of the topograph bordering the region labeled n then we obtain an equation $\Delta = h^2 - 4nk$ where h is the label on the edge and k is the label on the region on the opposite side of this edge. The equation $\Delta = h^2 - 4nk$ says that Δ is congruent to h^2 modulo $4n$. In case n is negative we interpret "modulo $4n$" to mean "modulo $4|n|$", but for the sake of simplicity we will still write "modulo $4n$".



This in fact gives an exact criterion for primitive representability:

Proposition. *Let two numbers n and Δ be given. Then the following two statements are equivalent*: (1) *There exists a form of discriminant Δ that represents n primitively.* (2) *Δ is congruent to a square modulo $4n$.*

Proof: As we saw above, if we have a form of discriminant Δ representing n primitively then we get an equation $\Delta = h^2 - 4nk$ for some integers h and k, and this equation says that Δ is the square of h modulo $4n$. Conversely, suppose that Δ is the square of some integer h modulo $4n$. This means that $h^2 - \Delta$ is an integer times $4n$, or in other words $h^2 - \Delta = 4nk$ for some k. This equation can be rewritten as $\Delta = h^2 - 4nk$. The three numbers n, h, and k can be used to construct a form whose topograph contains an edge with these three labels, for example the form $nx^2 + hxy + ky^2$, which has these three labels on the $1/0, 0/1$ edge. The discriminant of this form has the desired value $\Delta = h^2 - 4nk$. □

Let us see what this proposition implies for small values of n. For $n = 1$ it says that there is a form of discriminant Δ representing 1 if and only if Δ is a square modulo 4. The squares modulo 4 are 0 and 1, and we already know that discriminants of forms are always congruent to 0 or 1 modulo 4. So we conclude that for every possible value of the discriminant there exists a form that represents 1. This isn't

really new information, however, since the principal form x^2+dy^2 or $x^2+xy+dy^2$ represents 1 and there is a principal form for each discriminant.

In the next case $n=2$ we will get some new information. The possible values of the discriminant modulo 8 are $0,1,4,5$, and the squares modulo 8 are $0,1,4$ since $0^2=0$, $(\pm1)^2=1$, $(\pm2)^2=4$, $(\pm3)^2\equiv1$, and $(\pm4)^2\equiv0$. Thus 2 is not represented by any form of discriminant congruent to 5 modulo 8, but for all other values of the discriminant there is a form representing 2. Explicit forms are:

$$\Delta=8k: \quad 2x^2-ky^2$$
$$\Delta=8k+1: \quad 2x^2+xy-ky^2$$
$$\Delta=8k+4: \quad 2x^2+2xy-ky^2$$

For $n=3$ the discriminants modulo 12 are $0,1,4,5,8,9$ and the squares modulo 12 are $0,1,4,9$ since $0^2=0$, $(\pm1)^2=1$, $(\pm2)^2=4$, $(\pm3)^2=9$, $(\pm4)^2\equiv4$, $(\pm5)^2\equiv1$, and $(\pm6)^2\equiv0$. The excluded discriminants are those congruent to 5 or 8.

One could continue farther in this direction exploring which discriminants have forms representing a given number, but this is not really the question we want to answer, which is to start with a given discriminant, or even a given form, and decide which numbers it represents. The sort of answer we are looking for, based on the various examples we looked at earlier, is also a different sort of congruence condition, with congruence modulo the discriminant rather than congruence modulo $4n$. So there is more work to be done before we would have the sort of answer we want. Nevertheless, the representability criterion in the preceding proposition is the starting point.

Proof of Fermat's Theorem on Sums of Two Squares

Without a huge amount of extra work we can now settle the simplest case, the form x^2+y^2. Recall that the statement to be proved is that a number n is representable by the form x^2+y^2 if and only if it can be written as $n=m^2p_1\cdots p_k$ where each p_i is either 2 or a prime congruent to 1 modulo 4. The possibility that n is simply m^2 is allowed. Another way of stating the condition on n is to say that every prime factor $p=4k+3$ of n occurs to an even power, so it can be absorbed into the m^2 factor.

As a preliminary step to proving this, let us look at the condition in the preceding proposition for a number n to be primitively represented by x^2+y^2, which is that the discriminant -4 is a square modulo $4n$. This means that we have an equation $h^2=-4+4nk$ for some integers h and k. The number h must be even for this equation to hold, so $h=2l$ and the equation becomes $4l^2=-4+4nk$. Canceling the 4's, this becomes $l^2=-1+nk$. This just says that -1 is a square modulo n, so this is our new criterion for n to be primitively represented by x^2+y^2.

Now we begin the proof proper. First we show that if n is represented by the form x^2+y^2 then every prime factor $p=4k+3$ of n must occur to an even power in

n. Suppose on the contrary that we have a number n represented by x^2+y^2 whose prime factorization has a prime factor $p=4k+3$ occurring to an odd power. If this n is not primitively represented, we can cancel square factors of it until we get a new n represented primitively, with the same prime p still occurring to an odd power. Our representability criterion then says that -1 is a square modulo n. Since the prime $p=4k+3$ is a factor of n, this implies that -1 is a square modulo p. Applying the representability criterion in the reverse direction, this implies that p is represented (primitively) by x^2+y^2, so $p=x^2+y^2$ for some x and y. Since $p=4k+3$, if we look at the equation $p=x^2+y^2$ modulo 4, it says that 3 is the sum of two squares modulo 4. But this is impossible since the squares modulo 4 are 0 and 1 so adding two of them cannot give 3. This contradiction shows that primes $p=4k+3$ must occur in the prime factorization of n to an even power whenever n is represented by x^2+y^2.

To finish the proof of the theorem it suffices to prove two things:

(1) The primes $p=2$ and $p=4k+1$ are represented by x^2+y^2. (This is obvious for 2.)

(2) If two numbers m and n are represented by x^2+y^2 then so is their product mn.

The second statement is easier to prove so we do this first. Suppose m and n are represented as $m=a^2+b^2$ and $n=c^2+d^2$. Using complex numbers we can then factor m and n as $m=(a+bi)(a-bi)$ and $n=(c+di)(c-di)$. This gives a factorization of mn as a product of four factors, and by rearranging the factors we can obtain a representation of mn as a sum of two squares:

$$\begin{aligned}
mn &= (a^2+b^2)(c^2+d^2) \\
&= \big[(a+bi)(a-bi)\big]\big[(c+di)(c-di)\big] \\
&= \big[(a+bi)(c+di)\big]\big[(a-bi)(c-di)\big] \\
&= \big[(ac-bd)+(ad+bc)i\big]\big[(ac-bd)-(ad+bc)i\big] \\
&= (ac-bd)^2+(ad+bc)^2
\end{aligned}$$

The result of this calculation is the identity

$$(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2$$

which shows that the product of two numbers that are sums of two squares is again a sum of two squares. This identity can be checked directly without using complex numbers, just by multiplying both sides out, but the advantage of using complex numbers is that they show where the identity comes from.

It remains to prove the nontrivial part of the earlier statement (1), that every prime $p=4k+1$ is representable as the sum of two squares. Such a representation has to be primitive since p is prime. An equivalent statement is then that -1 is a square

modulo p, and this is what we will show by finding an explicit but rather large number h such that $h^2 \equiv -1$ modulo p.

Let us first illustrate how the proof will go by doing a specific example, the case $p = 13$, which is of the form $4k + 1$. Each of the numbers from 1 to $p - 1 = 12$ has a multiplicative inverse modulo 13:

$$1 \cdot 1 \equiv 1 \quad 2 \cdot 7 \equiv 1 \quad 3 \cdot 9 \equiv 1 \quad 4 \cdot 10 \equiv 1 \quad 5 \cdot 8 \equiv 1 \quad 6 \cdot 11 \equiv 1 \quad 12 \cdot 12 \equiv 1$$

The last congruence could have been written $(-1) \cdot (-1) \equiv 1$. The only cases when a number equals its own inverse modulo 13 are 1 and 12. Therefore if we consider the product

$$(p-1)! = 12! = (1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12)$$

all the terms that are not equal to their inverse will cancel in pairs, leaving only the last term 12. Thus we have the congruence $12! \equiv 12$ modulo 13, which we can rewrite as $12! \equiv -1$. Now notice that modulo 13 we have $7 \equiv -6$, $8 \equiv -5$, $9 \equiv -4$, etc., so we have

$$\begin{aligned} -1 &\equiv (1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12) \\ &\equiv (1)(2)(3)(4)(5)(6)(-6)(-5)(-4)(-3)(-2)(-1) \\ &= (6!)^2 \end{aligned}$$

This shows that -1 is a square modulo 13, namely $(6!)^2$. We will generalize this by showing that for every prime $p = 4k + 1$ the congruence $-1 \equiv [(2k)!]^2$ modulo p holds.

The first fact we need about congruences modulo a prime p is that each of the numbers $a = 1, 2, \cdots, p-1$ has a multiplicative inverse modulo p. To see why this is true, notice that each such a has no common factors with p, so we know from Chapter 2 that the equation $ax + py = 1$ has an integer solution (x, y). This equation can be rewritten as $ax \equiv 1$ modulo p, which says that x is an inverse for a modulo p. Note that any two choices for x here are congruent modulo p since if $ax \equiv 1$ and $ax' \equiv 1$ then multiplying both sides of $ax' \equiv 1$ by x gives $xax' \equiv x$, and $xa \equiv 1$ so we conclude that $x \equiv x'$.

Which numbers equal their own inverse modulo p? If $a \cdot a \equiv 1$, then we can rewrite this as $a^2 - 1 \equiv 0$, or in other words $(a+1)(a-1) \equiv 0$. This is certainly a valid congruence if $a \equiv \pm 1$, so suppose that $a \not\equiv \pm 1$. The factor $a + 1$ is then not congruent to 0 modulo p so it has a multiplicative inverse modulo p, and if we multiply the congruence $(a+1)(a-1) \equiv 0$ by this inverse, we get $a - 1 \equiv 0$ so $a \equiv 1$, contradicting the assumption that $a \not\equiv \pm 1$. This argument shows that the only numbers among $1, 2, \cdots, p-1$ that are congruent to their inverses modulo p are 1 and $p - 1$.

Now if we consider the product $(p-1)! = (1)(2)\cdots(p-1)$ modulo p, then each factor other than 1 and $p - 1$ can be paired up with its multiplicative inverse

and these two terms multiply together to give 1 modulo p, so the whole product simplifies to just $(1)(p-1)$. Thus we have a fact known as *Wilson's Theorem*:

$(p-1)! \equiv -1$ modulo p whenever p is prime.

Now let us assume that p is a prime of the form $p = 4k+1$. In the product $(p-1)!$ there are $p-1 = 4k$ terms. The first $2k$ of these are $(2k)!$ and the last $2k$, in reverse order, are $p-1, p-2, \cdots, p-2k$. Modulo p the latter are equivalent to $-1, -2, \cdots, -2k$, so we have

$$(p-1)! = (4k)! \equiv (1)(2)\cdots(2k-1)(2k)(-2k)(-(2k-1))\cdots(-2)(-1)$$

The last $2k$ of these factors are the negatives of the first $2k$ factors, and $2k$ is even, so the signs on all the negative terms cancel out and we see that $(p-1)!$ is congruent to $(2k)!\cdot(2k)!$ modulo p. Combining this with Wilson's theorem we get the desired result that -1 is a square modulo p, namely $-1 \equiv [(2k)!]^2$ modulo p. This finishes the proof of Fermat's theorem answering the question of which numbers are representable as sums of two squares.

Primes Representable in a Given Discriminant

For a given discriminant Δ, let us try to determine which primes are representable by some form of discriminant Δ. The more refined question would be to specify the form in advance as well, but as we have seen in examples, this makes the question quite subtle, so we only ask the weaker question of specifying the primes representable by at least one form of the given discriminant. The answer we are expecting is that these are, first of all, the "special" primes that divide Δ, and then for the remaining primes, the condition should be that it is the primes in certain congruence classes modulo $|\Delta|$.

All representations of a prime p must be primitive, so from our earlier discussion we have the criterion that p is representable by some form of discriminant Δ if and only if Δ is congruent to a square modulo $4p$. We can assume p is odd since for representability of $p = 2$ we already have the criterion that Δ is not congruent to 5 modulo 8. For odd p a small simplification is provided by the following:

Lemma. *For p odd, the condition that a discriminant Δ is congruent to a square modulo $4p$ is equivalent to Δ being a square modulo p.*

Proof: First assume that $\Delta \equiv h^2 \bmod 4p$ for some h. This means $\Delta - h^2$ is divisible by $4p$, hence $\Delta - h^2$ is divisible by p, which says that $\Delta \equiv h^2 \bmod p$.

For the converse we assume that $\Delta \equiv h^2 \bmod p$. We can assume that h has the same parity as Δ since if it does not, we simply replace h by $h+p$ which has the opposite parity from h since p is odd, and note that $(h+p)^2 \equiv h^2 \bmod p$. Since we always have $\Delta \equiv 0$ or $1 \bmod 4$, we must have $\Delta = 4k$ or $\Delta = 4k+1$, and since h has the same parity as Δ we have $h^2 = 4l$ or $h^2 = 4l+1$ in the two cases, respectively.

In either case $\Delta - h^2 = 4(k-l)$ so $\Delta - h^2$ is divisible by 4. It is also divisible by p by the assumption that $\Delta \equiv h^2 \bmod p$. Since p is odd, this implies that $\Delta - h^2$ is divisible by $4p$, so $\Delta \equiv h^2 \bmod 4p$, which finishes the proof of the converse. □

Now we can easily handle the special primes dividing Δ.

Proposition. *For each prime p that divides the discriminant Δ there exists a form of discriminant Δ that represents p.*

Proof: If p is an odd prime dividing Δ then $\Delta \equiv 0 \bmod p$ and 0 is a square mod p, namely 0^2, so the preceding lemma implies that Δ is a square mod $4p$ and hence p is represented by some form of discriminant Δ. For the prime 2, if this divides Δ then Δ is not 5 mod 8 so 2 is representable by some form of discriminant Δ. □

At this point it will be convenient to introduce some shorthand notation. For p an odd prime and a an integer not divisible by p, define the *Legendre symbol* $\left(\frac{a}{p}\right)$ by

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{if } a \text{ is not a square mod } p \end{cases}$$

Using this notation we can summarize our earlier results in the following way:

Proposition. *An odd prime p that does not divide Δ is representable by some form of discriminant Δ if and only if $\left(\frac{\Delta}{p}\right) = 1$.*

Typographical note. We will sometimes have occasion to multiply two or more Legendre symbols together, as in a product $\left(\frac{2}{7}\right)\left(\frac{3}{7}\right)$, which equals $(+1)(-1) = -1$. To distinguish this from simply multiplying the fractions $\frac{2}{7}$ and $\frac{3}{7}$ we will denote products of fractions by square brackets: $[\frac{2}{7}][\frac{3}{7}] = \frac{6}{49}$. In fact the only time we will have to multiply fractions is when their denominators are 2, whereas the Legendre symbol $\left(\frac{a}{p}\right)$ is only used for odd primes p, so the convention of using square brackets for fractions will not really be necessary.

The main tool we will use to compute $\left(\frac{\Delta}{p}\right)$ is the following famous theorem:

Quadratic Reciprocity. *If p and q are distinct odd primes then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless p and q are both congruent to 3 mod 4, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.*

This is a surprising statement because congruences modulo p and congruences modulo q generally have nothing to do with each other when p and q have no common factors, as is the case here with distinct primes. It is only on a special question like whether or not a number is a square modulo p or q that there is a connection. The principle of quadratic reciprocity was discovered in a more rudimentary form by Euler, and the final version given above was formulated by Legendre. The first person to prove it, however, was Gauss around 1797 or 1798. This is well over 100 years after Fermat, and it seems Fermat was not aware of quadratic reciprocity. Even though

Gauss's proof was correct, he was not satisfied that he understood quadratic reciprocity completely and later produced several different proofs. Since that time, many other proofs have been found. Many of them are elementary in the sense that they can be presented in a couple pages with no more background than we are assuming here, and we will present one such proof later in this chapter.

We will illustrate the use of quadratic reciprocity by four examples.

Example: $\Delta = 13$. First, since 13 is prime, the only special prime dividing Δ is 13 itself, so 13 is representable by a form of discriminant 13. The prime 2 is not representable since $\Delta = 13 \equiv 5 \bmod 8$. For odd primes $p \neq 13$ we have $\left(\frac{\Delta}{p}\right) = \left(\frac{13}{p}\right)$ and quadratic reciprocity says this equals $\left(\frac{p}{13}\right)$ since 13 is not congruent to 3 mod 4. Now it is easy to compute $\left(\frac{p}{13}\right)$ since the squares mod 13 are $(\pm1)^2 = 1$, $(\pm2)^2 = 4$, $(\pm3)^2 = 9$, $(\pm4)^2 = 16 \equiv 3$, $(\pm5)^2 = 25 \equiv 12$, and $(\pm6)^2 = 36 \equiv 10$. Thus the squares mod 13, apart from 0, are ±1, ±3, and ±4, so the primes representable by some form of discriminant 13 are 13 and the primes $p \equiv \pm1$, ±3, or ±4 mod 13. As it happens, the class number for discriminant 13 is one, as you can easily verify, so all forms of discriminant 13 are equivalent to the principal form $x^2 + xy - 3y^2$ and so we have an exact criterion for which primes this form represents: $p = 13$ and primes congruent to ±1, ±3, or ±4 mod 13. One could predict this was true by drawing a large enough part of the topograph, but a full proof requires more than this since it is obviously impossible to draw the whole topograph all at once and check all the infinitely many primes that occur in it. (For one thing, there is the difficulty of knowing when a large number is a prime.)

The full answer to which numbers, not just primes, are represented by the form $x^2 + xy - 3y^2$ is what you would now expect: The numbers $n = m^2 p_1 \cdots p_k$ where each p_i is 13 or a prime congruent to ±1, ±3, or ±4 modulo 13. The rest of the proof of this follows the same pattern as in the proof we gave for Fermat's theorem on the form $x^2 + y^2$. The only additional ingredient needed is a formula showing that the product of two numbers represented by $x^2 + xy - 3y^2$ is also represented by this form. The formula is not difficult and we will derive it in the next chapter for all principal forms.

In order to handle nonprime discriminants we need another general property of Legendre symbols:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

This will be proved later in the chapter when we prove quadratic reciprocity.

Example: $\Delta = 20$. The special primes 2 and 5 are representable by forms of discriminant 20. For other primes p we have $\left(\frac{\Delta}{p}\right) = \left(\frac{20}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. The squares mod 5, apart from 0, are 1 and 4, so the primes representable by forms of discriminant 20 are 2, 5, and primes congruent to ±1 mod 5. We could rephrase this in terms of congruence modulo the discriminant 20 by noting that the congru-

ence classes mod 20 that are not divisible by 2 or 5 (the special primes dividing 20) are $1,3,7,9,11,13,17,19$ and the only ones of these that are congruent to ±1 mod 5 are $1,9,11,19$, or in other words, ±1 and ±9 mod 20. Note that these are just the primes whose last digit is 1 or 9.

It is easy to check that there are exactly two equivalence classes of forms of discriminant 20, given by the forms x^2-5y^2 and $2x^2+2xy-2y^2 = 2(x^2+xy-y^2)$. The second form only represents even numbers, including 2, so the first form x^2-5y^2 must represent all the other primes, 5 and the primes with last digit 1 or 9.

Example: $\Delta = -15$. The special primes are 3 and 5, so these are representable. The prime 2 is representable since -15 is not congruent to 5 mod 8. For other primes p we have $\left(\frac{-15}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{5}{p}\right)$. From the proof of Fermat's theorem we know that

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{if } p = 4k+1 \\ -1 & \text{if } p = 4k+3 \end{cases}$$

Thus if $p = 4k+1$ we have $\left(\frac{-15}{p}\right) = (+1)\left(\frac{p}{3}\right)\left(\frac{p}{5}\right)$ and if $p = 4k+3$ we have $\left(\frac{-15}{p}\right) = (-1)\left[-\left(\frac{p}{3}\right)\right]\left(\frac{p}{5}\right)$, so in both cases we have $\left(\frac{-15}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{p}{5}\right)$. In order for this product to equal $+1$ it must either be $(+1)(+1)$ or $(-1)(-1)$. The congruence classes mod 15 we need to consider are $1,2,4,7,8,11,13,14$ (the numbers not divisible by 3 or 5). Looking at each of these eight cases in turn, we see that only the four cases $1,2,4,8$ give $\left(\frac{p}{3}\right)\left(\frac{p}{5}\right) = (+1)(+1)$ or $(-1)(-1)$. Thus the primes representable by forms of discriminant -15 are 3, 5, and primes congruent to $1,2,4,8$ mod 15. Note that this includes the prime 2 which we said was representable.

There are two equivalence classes of forms of discriminant -15, given by the forms $x^2+xy+4y^2$ and $2x^2+xy+2y^2$. If one draws a part of their topographs one can see that the two forms seem to be of different genera, with the first form representing primes congruent to 1 or 4 mod 15 and the second form representing the special primes 3 and 5 and primes congruent to 2 or 8 mod 15. However, we do not have the tools to prove this for all primes.

Example: $\Delta = -8$. Here there is only one form up to equivalence, the form x^2+2y^2. The only special prime is 2, and it is representable. For odd primes p we have $\left(\frac{-8}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^3 = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$. Since quadratic reciprocity as stated earlier only applies to odd primes, we do not yet have a way to compute $\left(\frac{2}{p}\right)$. This is given by the following formula that will be derived after we prove quadratic reciprocity:

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p = 8k \pm 1 \\ -1 & \text{if } p = 8k \pm 3 \end{cases}$$

Using this we can compute $\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ in each of the four cases $p \equiv 1,3,5,7$ mod 8, where the answers are, respectively, $(+1)(+1)$, $(-1)(-1)$, $(+1)(-1)$, and $(-1)(+1)$. We conclude that the primes representable by the form x^2+2y^2 are 2 and primes congruent to 1 or 3 mod 8.

Proof of Quadratic Reciprocity

First let us show that quadratic reciprocity can be expressed more concisely as a single formula

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{[\frac{p-1}{2}][\frac{q-1}{2}]} \qquad (*)$$

Here p and q are distinct odd primes. Since they are odd, the fractions $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are integers. The only way the exponent $[\frac{p-1}{2}][\frac{q-1}{2}]$ can be odd is for both factors to be odd, so $\frac{p-1}{2} = 2k+1$ and $\frac{q-1}{2} = 2l+1$. These equations can be rewritten as $p = 4k+3$ and $q = 4l+3$. Thus the only time that the right side of the formula $(*)$ can be -1 is when p and q are both congruent to 3 mod 4, and quadratic reciprocity is the assertion that the left side of $(*)$ has exactly this property.

There will be three main steps in the proof of quadratic reciprocity. The first is to derive an explicit algebraic formula for $\left(\frac{a}{p}\right)$ due originally to Euler. The second step is to use this formula to give a somewhat more geometric intrepretation of $\left(\frac{a}{p}\right)$ in terms of the number of dots in a certain triangular pattern. Then the third step is the actual proof of quadratic reciprocity using symmetry properties of the patterns of dots. This proof is due to Eisenstein, first published in 1844, simplifying an earlier proof by Gauss who was the first to give a full proof of quadratic reciprocity.

Step 1. In what follows we will always use p to denote an odd prime, and the symbol a will always denote an arbitrary nonzero integer not divisible by p. When we write a congruence such as $a \equiv b$ this will always mean congruence mod p, even if we do not explicitly say mod p.

Euler's formula is:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

For example, for $p = 11$ Euler's formula says $\left(\frac{2}{11}\right) = 2^5 = 32 \equiv -1 \mod 11$ and $\left(\frac{3}{11}\right) = 3^5 = 243 \equiv +1 \mod 11$. These are the correct values since the squares mod 11 are $(\pm1)^2 = 1$, $(\pm2)^2 = 4$, $(\pm3)^2 = 9$, $(\pm4)^2 \equiv 5$, and $(\pm5)^2 \equiv 3$.

Note that Euler's formula determines the value of $\left(\frac{a}{p}\right)$ uniquely since $+1$ and -1 are not congruent mod p since $p > 2$. It is not immediately obvious that the number $a^{\frac{p-1}{2}}$ should always be congruent to either $+1$ or -1 mod p, but when we prove Euler's formula we will see that this has to be true.

Taking $a = -1$ in Euler's formula gives the calculation $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ which equals $+1$ if $p = 4k+1$ and -1 if $p = 4k+3$, in agreement with what we showed earlier.

As a preliminary to proving Euler's formula let us prove the following congruence known as *Fermat's Little Theorem*:

$$a^{p-1} \equiv 1 \mod p \text{ whenever } p \text{ is an odd prime not dividing } a.$$

To see this, note first that the numbers $a, 2a, 3a, \cdots, (p-1)a$ are all distinct mod p since we know that a has a multiplicative inverse mod p, so in a congruence $ma \equiv na$ we can multiply both sides by the inverse of a to deduce that $m \equiv n$. Let us call this property that $ma \equiv na$ implies $m \equiv n$ the *cancellation property* for congruences mod p.

Thus the set $\{a, 2a, 3a, \cdots, (p-1)a\}$ is the same mod p as $\{1, 2, 3, \cdots, p-1\}$ since both sets have $p-1$ elements and neither set contains numbers that are 0 mod p. If we take the product of all the numbers in each of these two sets we obtain the congruence

$$(a)(2a)(3a)\cdots(p-1)a \equiv (1)(2)(3)\cdots(p-1) \mod p$$

We can cancel the factors $2, 3, \cdots, p-1$ from both sides by repeated applications of the cancellation property. The result is the congruence $a^{p-1} \equiv 1$ claimed by Fermat's Little Theorem.

Now we can prove Euler's formula for $\left(\frac{a}{p}\right)$. The first case is that $\left(\frac{a}{p}\right) = 1$, so a is a square mod p and $a \equiv x^2$ for some $x \not\equiv 0$. In this case we have $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1$ by Fermat's Little Theorem. So in this case Euler's formula $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ is valid, both sides being $+1$.

The other case is that $\left(\frac{a}{p}\right) = -1$ so a is not a square mod p. Observe first that the congruence $xy \equiv a$ has a solution y mod p for each $x \not\equiv 0$ since x has an inverse x^{-1} mod p so we can take $y = x^{-1}a$. Moreover the solution y is unique mod p since $xy_1 \equiv xy_2$ implies $y_1 \equiv y_2$ by the cancellation property. Since we are in the case that a is not a square mod p the solution y of $xy \equiv a$ satisfies $y \not\equiv x$. Thus the numbers $1, 2, 3, \cdots, p-1$ are divided up into $\frac{p-1}{2}$ pairs $\{x_1, y_1\}$, $\{x_2, y_2\}$, $\cdots$, $\{x_{\frac{p-1}{2}}, y_{\frac{p-1}{2}}\}$ with $x_i y_i \equiv a$ for each i. Multiplying all these $\frac{p-1}{2}$ pairs together, we get

$$a^{\frac{p-1}{2}} \equiv x_1 y_1 x_2 y_2 \cdots x_{\frac{p-1}{2}} y_{\frac{p-1}{2}}$$

The product on the right is just a rearrangement of $(1)(2)(3)\cdots(p-1)$, and Wilson's Theorem says that this product is congruent to -1 mod p. Thus we see that Euler's formula $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ holds also when $\left(\frac{a}{p}\right) = -1$, completing the proof in both cases.

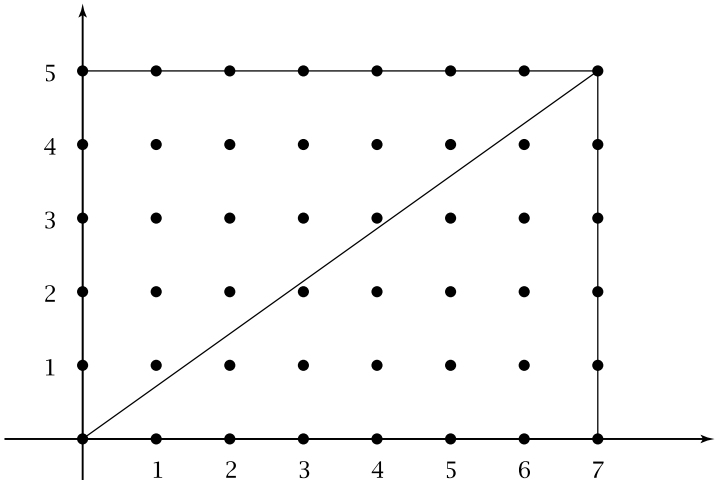
A consequence of Euler's formula is the multiplicative property of Legendre symbols that we stated and used earlier in the chapter:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

This holds since $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}$.

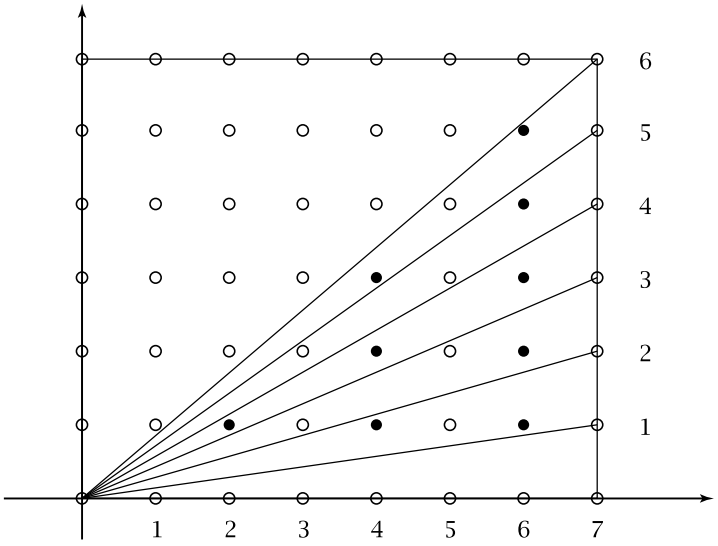
Step 2. Here our aim is to express the Legendre symbol $\left(\frac{a}{p}\right)$ in more geometric terms. To begin, consider a rectangle in the first quadrant of the xy-plane that is p units wide and a units high, with one corner at the origin and the opposite corner at the

point (p, a). We will be interested in points that lie strictly in the interior of the rectangle and whose coordinates are integers. Points satisfying the latter condition are called *lattice points*. The number of lattice points in the interior is then $(p-1)(a-1)$ since their x-coordinates can range from 1 to $p-1$ and their y-coordinates from 1 to $a-1$, independently.



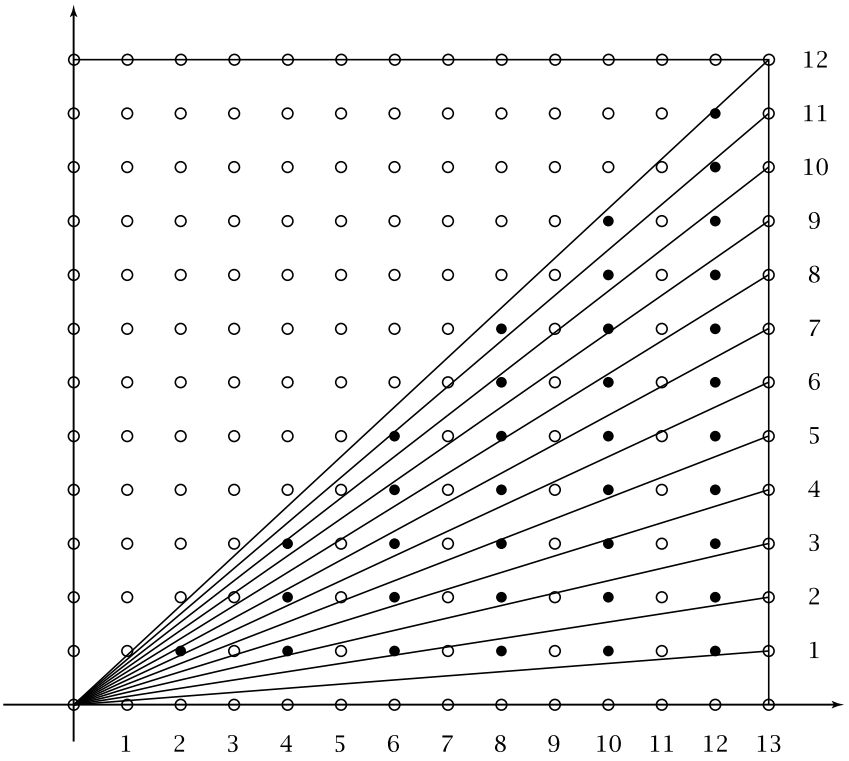
The diagonal of the rectangle from $(0,0)$ to (p,a) does not pass through any of these interior lattice points since we assume that the prime p does not divide a, so the fraction a/p, which is the slope of the diagonal, is in lowest terms. (If there were an interior lattice point on the diagonal, the slope of the diagonal would be a fraction with numerator and denominator smaller than a and p.) Since there are no interior lattice points on the diagonal, exactly half of the lattice points inside the rectangle lie on each side of the diagonal, so the number of lattice points below the diagonal is $\frac{1}{2}(p-1)(a-1)$. This is an integer since p is odd, which makes $p-1$ even.

A more refined question one can ask is how many lattice points below the diagonal have even x-coordinate and how many have odd x-coordinate. Here there is no guarantee that these two numbers must be equal, and indeed if they were equal then the number would be $\frac{1}{4}(p-1)(a-1)$ but this fraction does not have to be an integer, for example when $p=7$ and $a=4$. We denote the number of lattice points below the diagonal with even x-coordinate by the letter e. Here is a figure showing the values of e when $p=7$ and a ranges from 1 to 6:



a	e	$\left(\frac{a}{7}\right)$
6	9	–1
5	7	–1
4	6	+1
3	3	–1
2	2	+1
1	0	+1

A slightly more complicated example is when $p = 13$ and a goes from 1 to 12:



a	e	$\left(\frac{a}{13}\right)$
12	36	+1
11	33	–1
10	30	+1
9	26	+1
8	23	–1
7	21	–1
6	15	–1
5	13	–1
4	10	+1
3	6	+1
2	3	–1
1	0	+1

The way that e varies with a seems somewhat unpredictable. What we will show is that just knowing the parity of e is already enough to determine the value of the Legendre symbol via the formula

$$\left(\frac{a}{p}\right) = (-1)^e$$

To prove this we first derive a formula for e. The segment of the vertical line $x = u$ going from the x-axis up to the diagonal has length ua/p since the slope of the diagonal is a/p. If u is a positive integer the number of lattice points on this line segment is $\lfloor \frac{ua}{p} \rfloor$, the greatest integer $n \le \frac{ua}{p}$. Now if we add up these numbers of lattice points for u running through the set of even numbers $E = \{2, 4, \cdots, p-1\}$

we get

$$e = \sum_E \left\lfloor \frac{ua}{p} \right\rfloor$$

The way to compute $\lfloor \frac{ua}{p} \rfloor$ is to apply the division algorithm for integers, dividing p into ua to obtain $\lfloor \frac{ua}{p} \rfloor$ as the quotient with a remainder that we denote $r(u)$. Thus we have the formula

$$ua = p\left\lfloor \frac{ua}{p} \right\rfloor + r(u) \tag{1}$$

This formula implies that the number $\lfloor \frac{ua}{p} \rfloor$ has the same parity as $r(u)$ since u is even and p is odd. This relation between parities implies that the number $(-1)^e$ that we are interested in can also be computed as

$$(-1)^e = (-1)^{\sum_E \lfloor \frac{ua}{p} \rfloor} = (-1)^{\sum_E r(u)} \tag{2}$$

With this last expression in mind we will focus our attention on the remainders $r(u)$.

The number $r(u)$ lies strictly between 0 and p and can be either even or odd, but in both cases we can say that $(-1)^{r(u)}r(u)$ is congruent to an even number in the interval $(0, p)$ since if $r(u)$ is odd, so is $(-1)^{r(u)}r(u)$ and then adding p to this gives an even number between 0 and p. Thus there is always an even number $s(u)$ between 1 and p that is congruent to $(-1)^{r(u)}r(u)$ mod p. Obviously $s(u)$ is unique since no two numbers in $(0, p)$ are congruent mod p.

A key fact about these even numbers $s(u)$ is that they are all distinct as u varies over the set E. For suppose we have $s(u) = s(v)$ for another even number v in E. Thus $r(u) \equiv \pm r(v)$ mod p, which implies $au \equiv \pm av$ mod p in view of the equation (1) above. We can cancel the a from both sides of this congruence to get $u \equiv \pm v$. However we cannot have $u \equiv -v$ because the number between 0 and p that is congruent to $-v$ is $p - v$, so we would have $u = p - v$ which is impossible since u and v are even while p is odd. Thus we must have $u \equiv +v$, hence $u = v$ since these are numbers strictly between 0 and p. This shows that the numbers $s(u)$ are all distinct.

Now consider the product of all the numbers $(-1)^{r(u)}r(u)$ as u ranges over the set E. Written out, this is

$$\Big[(-1)^{r(2)}r(2)\Big]\Big[(-1)^{r(4)}r(4)\Big]\cdots\Big[(-1)^{r(p-1)}r(p-1)\Big] \tag{3}$$

By equation (1) we have $r(u) \equiv ua$ mod p, so this product is congruent mod p to

$$\Big[(-1)^{r(2)}2a\Big]\Big[(-1)^{r(4)}4a\Big]\cdots\Big[(-1)^{r(p-1)}(p-1)a\Big]$$

On the other hand, by the definition of the numbers $s(u)$ the product (3) is congruent mod p to

$$[s(2)][s(4)]\cdots[s(p-1)]$$

There are $\frac{p-1}{2}$ factors here and they are all distinct even numbers in the interval $(0, p)$ as we showed in the previous paragraph, so they are just a rearrangement of the numbers $2, 4, \cdots, p-1$. Thus we have the congruence

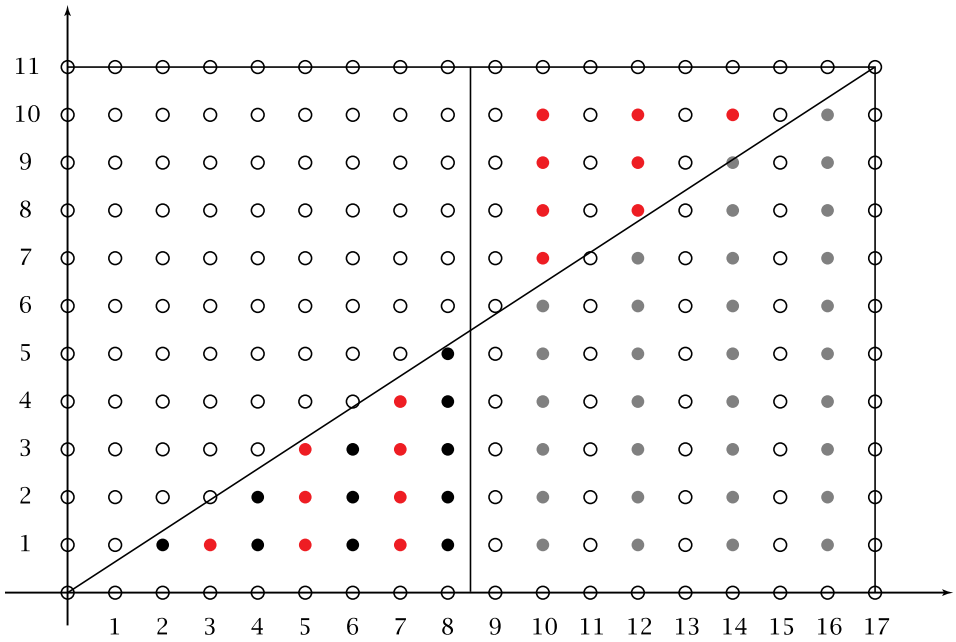
$$\Big[(-1)^{r(2)}2a\Big]\Big[(-1)^{r(4)}4a\Big]\cdots\Big[(-1)^{r(p-1)}(p-1)a\Big] \equiv (2)(4)\cdots(p-1) \mod p$$

We can cancel the factors $2, 4, \cdots, p-1$ from both sides of this congruence to obtain

$$(-1)^{\sum_E r(u)} a^{\frac{p-1}{2}} \equiv 1 \mod p$$

Both the factors $(-1)^{\sum_E r(u)}$ and $a^{\frac{p-1}{2}}$ are ± 1 mod p and their product is 1 so they must be equal mod p (using the fact that 1 and -1 are not congruent modulo an odd prime). By Euler's formula we have $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$, so from the earlier formula (2) we conclude that $\left(\frac{a}{p}\right) = (-1)^e$. This finishes Step 2 in the proof of quadratic reciprocity.

Step 3. Now we specialize the value of a to be an odd prime q distinct from p. As in Step 2 we consider a $p \times q$ rectangle. We know that $\left(\frac{q}{p}\right) = (-1)^e$ where e is the number of lattice points with even x-coordinate inside the rectangle and below the diagonal. Suppose that we divide the rectangle into two equal halves separated by the vertical line $x = \frac{p}{2}$. This line does not pass through any lattice points since p is odd. This vertical line cuts off two smaller triangles from the two large triangles above and below the diagonal of the rectangle. Call the lower small triangle L and the upper one U, and let l and u denote the number of lattice points with even x-coordinate in L and U respectively. We note that u has the same parity as the number of lattice points with even x-coordinate in the quadrilateral below U in the right half of the rectangle since each column of lattice points in the rectangle has $q-1$ points, an even number. Thus e has the same parity as $l+u$, hence $(-1)^e = (-1)^{l+u}$.



The next thing to notice is that rotating the triangle U by 180 degrees about the center of the rectangle carries it onto the triangle L. This rotation takes the lattice points in U with even x-coordinate onto the lattice points in L with odd x-coordinate. Thus we obtain the formula $\left(\frac{q}{p}\right) = (-1)^t$ where t is the total number of lattice points in the triangle L.

Reversing the roles of p and q, we can also say that $\left(\frac{p}{q}\right) = (-1)^{t'}$ where t' is the number of lattice points in the triangle L' above the diagonal and below the horizontal line $y = \frac{q}{2}$ bisecting the rectangle. Then $t + t'$ is the number of lattice points in the small rectangle formed by L and L' together. This number is just $[\frac{p-1}{2}][\frac{q-1}{2}]$. Thus we have

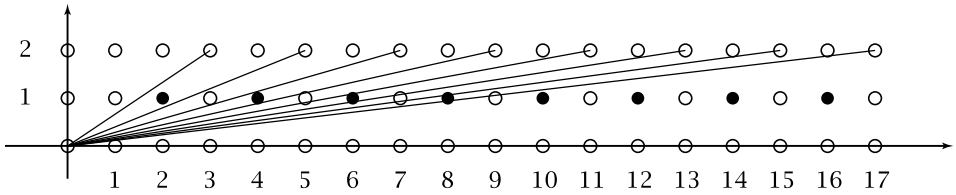
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^t(-1)^{t'} = (-1)^{t+t'} = (-1)^{[\frac{p-1}{2}][\frac{q-1}{2}]}$$

which finally finishes the proof of quadratic reciprocity.

We can also use the geometric interpretation of $\left(\frac{a}{p}\right)$ to prove the formula for $\left(\frac{2}{p}\right)$ that was stated earlier in this chapter, namely

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p = 8k \pm 1 \\ -1 & \text{if } p = 8k \pm 3 \end{cases}$$

We have shown that $\left(\frac{2}{p}\right) = (-1)^e$ where e is the number of lattice points inside a $p \times 2$ rectangle lying below the diagonal and having even x coordinate, as indicated in the following figure which shows the diagonals for $p = 3, 5, 7, \cdots, 17$:



p	3	5	7	9	11	13	15	17
e	1	1	2	2	3	3	4	4

Another way to describe e is to say that it is equal to the number of even integers in the interval from $p/2$ to p. We do not need to assume that p is prime in order to count these points below the diagonals, just that p is odd. One can see what the pattern is just by looking at the figure: Each time p increases by 2 there is one more even number at the right end of the interval $(p/2, p)$, and there may or may not be one fewer even number at the left end of the interval, depending on whether p is increasing from $4k-1$ to $4k+1$ or from $4k+1$ to $4k+3$. It follows that the parity of e depends only on the value of p mod 8 as in the table for $p \le 17$, so e is even for $p \equiv \pm 1 \bmod 8$ and e is odd for $p \equiv \pm 3 \bmod 8$.

Exercises

1. For the form $Q(x,y) = x^2 + xy + y^2$ do the following things:
(a) Draw enough of the topograph to show all the values less than 100 that occur in the topograph. You do not need to draw parts of the topograph that are symmetric with other parts.
(b) Make a list of the primes less than 100 that occur in the topograph, and a list of the primes less than 100 that do not occur.
(c) Characterize the primes in the two lists in part (b) in terms of congruence classes modulo $|\Delta|$ where Δ is the discriminant of Q.
(d) Characterize the nonprime values in the topograph in terms of their factorizations into primes in the lists in part (b).
(e) Summarize the previous parts by giving a simple criterion for which numbers are representable by the form Q, i.e., the numbers n such that $Q(x,y) = n$ has an integer solution (x,y), primitive or not. The criterion should say something like n is representable if and only if $n = m^2 p_1 \cdots p_k$ where each p_i is a prime such that ...
(e) Check that all forms having the same discriminant as Q are equivalent to Q.

2. Do the same things for the form $x^2 + xy - y^2$. This form is hyperbolic and it takes the same negative values as positive values, so you can just ignore all the negative values.

3. Do the same things for the form $x^2 + xy + 2y^2$, except that this time you only need to consider values less than 50 instead of 100.

4. For discriminant $\Delta = -24$ do the following:
(a) Verify that the class number is 2 and find two quadratic forms Q_1 and Q_2 of discriminant -24 that are not equivalent.
(b) Draw topographs for Q_1 and Q_2 showing all values less than 100. (You don't have to repeat parts of the topographs that are symmetric.)
(c) Divide the primes less than 100 into three lists: those represented by Q_1, those represented by Q_2, and those represented by neither Q_1 nor Q_2. (No primes are represented by both Q_1 and Q_2.)
(d) Characterize the primes in the three lists in part (c) in terms of congruence classes modulo $|\Delta| = 24$.
(e) Characterize the nonprime values in the topograph of Q_1 in terms of their factorizations into primes in the lists in part (c), and then do the same thing for Q_2. Your answers should be in terms of whether there are an even or an odd number of prime factors from certain of the lists.
(f) Summarize the previous parts by giving a criterion for which numbers are representable by the form Q_1 and which are representable by Q_2.

5. This problem will show how things can be more complicated than in the previous problems.

(a) Show that the class number for discriminant -23 is 2 and find forms Q_1 and Q_2 of discriminant -23 that are not equivalent.
(b) Draw the topographs of Q_1 and Q_2 up to the value 70. (Again you don't have to repeat symmetric parts.)
(c) Find a number n that occurs in both topographs, and find the x and y values that give $Q_1(x_1, y_1) = n = Q_2(x_2, y_2)$. (This sort of thing never happens in the previous problems.)
(d) Find a prime p_1 in the topograph of Q_1 and a different prime p_2 in the topograph of Q_2 such that p_1 and p_2 are congruent modulo $|\Delta| = 23$. (This sort of thing also never happens in the previous problems.)

6. As a sort of converse to Wilson's theorem, show that if n is not a prime then $(n-1)!$ is not congruent to -1 mod n. More precisely, when $n > 4$ and n is not prime, show that n divides $(n-1)!$, so $(n-1)! \equiv 0 \bmod n$. What happens when $n = 4$?

7. Determine the values of Δ for which there exists a quadratic form of discriminant Δ that represents 5, and also determine the discriminants Δ for which there does not exist a form representing 5.

8. Verify that the statement of quadratic reciprocity is true for the following pairs of primes (p, q): $(3,5)$, $(3,7)$, $(3,13)$, $(5,13)$, $(7,11)$, and $(13,17)$.

9. (a) There is an example near the end of this chapter that works out which primes are represented by some form of discriminant 13, using quadratic reciprocity for the key step. Do the same thing for discriminant 17.
(b) Show that all forms of discriminant 17 are equivalent to the principal form $x^2 + xy - 4y^2$.
(c) Draw enough of the topograph of $x^2 + xy - 4y^2$ to show all values between -70 and 70, and verify that the primes that occur are precisely the ones predicted by your answer in part (a).

10. Using quadratic reciprocity as in part (a) of the previous problem, figure out which primes are represented by at least one form of discriminant Δ for the following values of Δ: -3, 8, -20, 21.

11. (a) Repeat the previous problem for $\Delta = 9$ where the answer may be rather surprising. Note that quadratic forms with $\Delta = 9$ are 0-hyperbolic, rather than the more usual hyperbolic or elliptic forms that we consider. (0-hyperbolic forms factor into linear factors with integer coefficients.)
(b) Draw enough of the topographs of all three equivalence classes of forms with $\Delta = 9$ to see why the answer you got in part (a) is correct.
(c) Show that in fact *every* integer n is represented primitively by at least one quadratic form of discriminant 9.

Quadratic Fields

Even when one's primary interest is in integer solutions to equations, it can sometimes be very helpful to consider more general sorts of numbers. For example, when studying the principal quadratic form $x^2 - Dy^2$ of discriminant $4D$ it can be a great aid to understanding to allow ourselves to factor this form as $(x + y\sqrt{D})(x - y\sqrt{D})$. Here we allow D to be negative as well as positive, in which case we would be moving into the realm of complex numbers.

To illustrate this idea, consider the case $D = -1$, so the form is $x^2 + y^2$ which we are factoring as $(x + yi)(x - yi)$. Writing a number n as a sum $a^2 + b^2$ is then equivalent to factoring it as $(a + bi)(a - bi)$. For example $5 = 2^2 + 1^2 = (2 + i)(2 - i)$, and $13 = 3^2 + 2^2 = (3 + 2i)(3 - 2i)$, so 5 and 13 are no longer prime when we allow factorizations using numbers $a + bi$. Sometimes a nonprime number such as 65 can be written as the sum of two squares in more than one way: $65 = 8^2 + 1^2 = 4^2 + 7^2$, so it has factorizations as $(8 + i)(8 - i)$ and $(4 + 7i)(4 - 7i)$. This becomes more understandable if one uses the factorization

$$65 = 5 \cdot 13 = (2 + i)(2 - i)(3 + 2i)(3 - 2i)$$

If we combine these four terms as $(2 - i)(3 + 2i) = 8 + i$ and $(2 + i)(3 - 2i) = 8 - i$ we get the representation $65 = 8^2 + 1^2 = (8 + i)(8 - i)$, whereas if we combine them as $(2 + i)(3 + 2i) = 4 + 7i$ and $(2 - i)(3 - 2i) = 4 - 7i$ we get the other representation $65 = 4^2 + 7^2 = (4 + 7i)(4 - 7i)$.

Thus we will consider the set

$$\mathbb{Z}[\sqrt{D}] = \{ x + y\sqrt{D} \mid x, y \in \mathbb{Z} \}$$

which consists of real numbers if $D > 0$ and complex numbers if $D < 0$. We will always assume D is not a square, so $\mathbb{Z}[\sqrt{D}]$ is not just $\mathbb{Z}$. When $D = -1$ we have $\mathbb{Z}[\sqrt{D}] = \mathbb{Z}[i]$, and numbers $a + bi$ in $\mathbb{Z}[i]$ are known as *Gaussian integers*.

Primes and Units

We will be interested in factorizations of numbers in $\mathbb{Z}[\sqrt{D}]$, particularly how they factor into 'primes'. If a prime p in $\mathbb{Z}$ happens to be representable as $p = x^2 - Dy^2$ then this is saying that p is no longer prime in $\mathbb{Z}[\sqrt{D}]$ since it factors as $p = (x + y\sqrt{D})(x - y\sqrt{D})$. Of course, we should say precisely what we mean by a 'prime' in $\mathbb{Z}[\sqrt{D}]$. For an ordinary integer $p > 1$, being prime means that p is divisible only by itself and 1. If we allow negative numbers, we can "factor" a prime p as $(-1)(-p)$, but this should not count as a genuine factorization, otherwise there would be no primes at all in $\mathbb{Z}$. In $\mathbb{Z}[\sqrt{D}]$ things can be a little more complicated because of the existence of *units* in $\mathbb{Z}[\sqrt{D}]$, the nonzero elements $\varepsilon \in \mathbb{Z}[\sqrt{D}]$ whose inverse ε^{-1} also lies in $\mathbb{Z}[\sqrt{D}]$. For example, in the Gaussian integers $\mathbb{Z}[i]$ there are four obvious units, ± 1 and $\pm i$, since $(i)(-i) = 1$. We will see in a little while that these

are the only units in $\mathbb{Z}[i]$. Having four units in $\mathbb{Z}[i]$ instead of just ± 1 complicates the factorization issue slightly, but not excessively so.

For positive values of D things are somewhat less tidy because there are always infinitely many units in $\mathbb{Z}[\sqrt{D}]$ when $D > 0$. For example, when $D = 2$ the number $\varepsilon = 3 + 2\sqrt{2}$ is a unit because $(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1$. All the powers of $3 + 2\sqrt{2}$ are therefore also units, and there are infinitely many of them since $3 + 2\sqrt{2} > 1$ so $(3 + 2\sqrt{2})^n \to \infty$ as $n \to \infty$.

Whenever ε is a unit in $\mathbb{Z}[\sqrt{D}]$ we can factor any other number α in $\mathbb{Z}[\sqrt{D}]$ as $\alpha = (\alpha\varepsilon)(\varepsilon^{-1})$. If we allowed this as a genuine factorization there would be no primes in $\mathbb{Z}[\sqrt{D}]$, so it is best not to consider it as a genuine factorization. This leads us to the following definition:

> An element α of $\mathbb{Z}[\sqrt{D}]$ is said to be *prime* in $\mathbb{Z}[\sqrt{D}]$ if it is neither 0 nor a unit, and if whenever we have a factorization of α as $\alpha = \beta\gamma$ with both β, γ in $\mathbb{Z}[\sqrt{D}]$, then it must be the case that either β or γ is a unit in $\mathbb{Z}[\sqrt{D}]$.

Not allowing units as primes is analogous to the standard practice of not considering 1 to be a prime in $\mathbb{Z}$.

If we replace $\mathbb{Z}[\sqrt{D}]$ by $\mathbb{Z}$ in the definition of primeness above, we get the condition that an integer a in $\mathbb{Z}$ is prime if its only factorizations are the trivial ones $a = (a)(1) = (1)(a)$ and $a = (-a)(-1) = (-1)(-a)$, which is what we would expect. This definition of primeness also means that we are allowing negative primes as the negatives of the positive primes in $\mathbb{Z}$.

A word of caution: An integer p in $\mathbb{Z}$ can be prime in $\mathbb{Z}$ but not prime in $\mathbb{Z}[\sqrt{D}]$. For example, in $\mathbb{Z}[i]$ we have the factorization $5 = (2 + i)(2 - i)$, and as we will be able to verify soon, neither $2 + i$ nor $2 - i$ is a unit in $\mathbb{Z}[i]$. Hence by our definition 5 is not a prime in $\mathbb{Z}[i]$, even though it is prime in $\mathbb{Z}$. Thus one always has to be careful when speaking about primeness to distinguish "prime in $\mathbb{Z}$" from "prime in $\mathbb{Z}[\sqrt{D}]$".

Having defined what we mean by primes in $\mathbb{Z}[\sqrt{D}]$ we can now ask the fundamental questions that will be central to this chapter:

> *Does every element of $\mathbb{Z}[\sqrt{D}]$, apart from 0 and units, have a factorization into primes in $\mathbb{Z}[\sqrt{D}]$? And if it does, is this factorization unique?*

The uniqueness question needs a little explanation. If we have a unit ε in $\mathbb{Z}[\sqrt{D}]$ we can always modify a factorization $\alpha = \beta\gamma$ to give other factorizations $\alpha = (\varepsilon\beta)(\varepsilon^{-1}\gamma)$ and $\alpha = (\varepsilon^{-1}\beta)(\varepsilon\gamma)$. This is analogous to writing $6 = (2)(3) = (-2)(-3)$ in $\mathbb{Z}$. This sort of nonuniqueness is unavoidable, but it is also not too serious a problem. So when we speak of factorization in $\mathbb{Z}[\sqrt{D}]$ being unique, we will always mean unique up to insertion of units (and their inverses).

The Norm

We introduce now a basic tool that is of great use in studying factorizations. For a number $x + y\sqrt{D}$ define its *norm* to be

$$N(x + y\sqrt{D}) = (x + y\sqrt{D})(x - y\sqrt{D}) = x^2 - Dy^2$$

Thus the norm is a function $N : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}$. The main reason the norm is important is because of the following multiplicativity property:

Proposition. *$N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$.*

Proof: This is simply a calculation. Let $\alpha = a + b\sqrt{D}$ and $\beta = c + d\sqrt{D}$. Then $\alpha\beta = (ac + bdD) + (ad + bc)\sqrt{D}$ and hence

$$\begin{aligned} N(\alpha\beta) &= a^2c^2 + 2abcdD + b^2d^2D^2 - (a^2d^2 + b^2c^2 + 2abcd)D \\ &= a^2c^2 + b^2d^2D^2 - a^2d^2D - b^2c^2D \end{aligned}$$

On the other hand we have

$$\begin{aligned} N(\alpha)N(\beta) &= (a^2 - b^2D)(c^2 - d^2D) \\ &= a^2c^2 + b^2d^2D^2 - a^2d^2D - b^2c^2D \end{aligned}$$

So $N(\alpha\beta) = N(\alpha)N(\beta)$. □

The multiplicative property $N(\alpha\beta) = N(\alpha)N(\beta)$ implies that if two integers m and n are represented by the form $x^2 - Dy^2$, then so is their product mn. In the case of the form $x^2 + y^2$ this fact played a role in our proof of Fermat's theorem in the previous chapter, so now we see how this fits into a more general picture.

Using the multiplicative property of the norm we can derive a simple criterion for recognizing units:

Proposition. *An element $\varepsilon \in \mathbb{Z}[\sqrt{D}]$ is a unit if and only if $N(\varepsilon) = \pm 1$.*

Proof: Suppose ε is a unit, so its inverse ε^{-1} also lies in $\mathbb{Z}[\sqrt{D}]$. Then we have $N(\varepsilon)N(\varepsilon^{-1}) = N(\varepsilon\varepsilon^{-1}) = N(1) = 1$. Since both $N(\varepsilon)$ and $N(\varepsilon^{-1})$ are elements of $\mathbb{Z}$, this forces $N(\varepsilon)$ to be ± 1. Conversely, the inverse of an element $\varepsilon = a + b\sqrt{D}$ in $\mathbb{Z}[\sqrt{D}]$ is $\varepsilon^{-1} = (a - b\sqrt{D})/N(\varepsilon)$ since multiplying this by $a + b\sqrt{D}$ gives 1. Hence if $N(\varepsilon) = \pm 1$ we have $\varepsilon^{-1} = \pm(a - b\sqrt{D})$, an element of $\mathbb{Z}[\sqrt{D}]$, so ε is a unit. □

When D is negative there are very few units in $\mathbb{Z}[\sqrt{D}]$ since in these cases the equation $N(x + y\sqrt{D}) = x^2 - Dy^2 = \pm 1$ has very few integer solutions, namely, if $D = -1$ there are only the four solutions $(x, y) = (\pm 1, 0)$ and $(0, \pm 1)$ while if $D < -1$ there are only the two solutions $(x, y) = (\pm 1, 0)$. Thus the only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$, and the only units in $\mathbb{Z}[\sqrt{D}]$ for $D < -1$ are ± 1.

The situation for $\mathbb{Z}[\sqrt{D}]$ with D positive is quite different. Here we are looking for solutions of $x^2 - Dy^2 = \pm 1$ with $D > 0$. This is Pell's equation, and we know

from our study of topographs of hyperbolic forms that the equation $x^2 - Dy^2 = 1$ has infinitely many solutions since the value 1 occurs along the periodic separator line in the topograph of $x^2 - Dy^2$ when $(x, y) = (1, 0)$, so it appears infinitely often by periodicity. For some values of D the number -1 also appears along the separator line, and then it too appears infinitely often. Thus $\mathbb{Z}[\sqrt{D}]$ has infinitely many units $\varepsilon = x + y\sqrt{D}$, with arbitrarily large values of x and y. Fortunately the situation turns out to be not so bad as it seems at first glance:

Proposition. *The units in $\mathbb{Z}[\sqrt{D}]$, when $D > 0$, are the elements $\pm\varepsilon^n$ for $n \in \mathbb{Z}$, where $\varepsilon = p + q\sqrt{D}$ and (p, q) is the smallest positive solution of $x^2 - Dy^2 = \pm 1$.*

The unit $p + q\sqrt{D}$ given by this proposition is called the *fundamental unit*.

Proof: We know from Chapter 4 that the translation or glide-reflection symmetry along the separator line for $x^2 - Dy^2$ is given by the transformation

$$\begin{pmatrix} p & Dq \\ q & p \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} px + Dqy \\ qx + py \end{pmatrix}$$

On the other hand, we also have

$$(p + q\sqrt{D})(x + y\sqrt{D}) = (px + Dqy) + (qx + py)\sqrt{D}$$

which is really the same transformation of the coefficients x and y. The units in $\mathbb{Z}[\sqrt{D}]$ are exactly the elements $x + y\sqrt{D}$ satisfying $x^2 - Dy^2 = \pm 1$, and we know that the solutions of this equation are exactly the pairs $\binom{x}{y}$ obtainable as products

$$\pm \begin{pmatrix} px + Dqy \\ qx + py \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

as n ranges over $\mathbb{Z}$. Hence the units are exactly the elements $\pm\varepsilon^n$ times 1. □

Another basic application of the norm is the following useful fact:

Proposition. *Let α be an element of $\mathbb{Z}[\sqrt{D}]$. If $N(\alpha)$ is prime in $\mathbb{Z}$ then α is prime in $\mathbb{Z}[\sqrt{D}]$.*

For example, when we factor 5 as $(2 + i)(2 - i)$ in $\mathbb{Z}[i]$, this proposition implies that both factors are prime since the norm of each one is 5, which is prime in $\mathbb{Z}$.

Proof: Suppose an element $\alpha \in \mathbb{Z}[\sqrt{D}]$ has a factorization $\alpha = \beta\gamma$, hence $N(\alpha) = N(\beta)N(\gamma)$. If $N(\alpha)$ is prime in $\mathbb{Z}$, this forces one of $N(\beta)$ and $N(\gamma)$ to be ± 1, hence one of β and γ is a unit. This means α is a prime since it cannot be 0 or a unit, as its norm is a prime. □

The converse of this proposition is not generally true. For example the number 3 has norm 9, which is not prime in $\mathbb{Z}$, and yet 3 is prime in $\mathbb{Z}[i]$ since if we had a factorization $3 = \alpha\beta$ in $\mathbb{Z}[i]$ with neither α nor β a unit, then the equation

$N(\alpha)N(\beta) = N(3) = 9$ would imply that $N(\alpha) = \pm 3 = N(\beta)$, but there are no elements of $\mathbb{Z}[i]$ with norm ± 3 since the equation $x^2+y^2 = \pm 3$ has no integer solutions.

Prime Factorizations

Now we can prove that prime factorizations always exist:

Proposition. *Every nonzero element of $\mathbb{Z}[\sqrt{D}]$ that is not a unit can be factored as a product of primes in $\mathbb{Z}[\sqrt{D}]$.*

Proof: We argue by induction on $|N(\alpha)|$. Since we are excluding 0 and units, the induction starts with the case $|N(\alpha)| = 2$. In this case α must itself be a prime by the preceding proposition, since 2 is prime in $\mathbb{Z}$. For the induction step, if α is a prime there is nothing to prove. If α is not prime, it factors as $\alpha = \beta\gamma$ with neither β nor γ a unit, so $|N(\beta)| > 1$ and $|N(\gamma)| > 1$. Since $N(\alpha) = N(\beta)N(\gamma)$, it follows that $|N(\beta)| < |N(\alpha)|$ and $|N(\gamma)| < |N(\alpha)|$. By induction, both β and γ are products of primes in $\mathbb{Z}[\sqrt{D}]$, hence their product α is also a product of primes. □

Let us investigate how to compute a prime factorization by looking at the case of $\mathbb{Z}[i]$, the Gaussian integers. Assuming that factorizations of Gaussian integers into primes are unique (up to units), which we will prove later, here is a procedure for finding the prime factorization of a Gaussian integer $\alpha = a + bi$:

(1) Factor the integer $N(\alpha) = a^2 + b^2$ into primes p_k in $\mathbb{Z}$.
(2) Determine how each p_k factors into primes in $\mathbb{Z}[i]$.
(3) By the uniqueness of prime factorizations, the primes found in step (2) will be factors of either $a+bi$ or $a-bi$ since they are factors of $(a+bi)(a-bi)$, so all that remains is to test which of the prime factors of each p_k are factors of $a+bi$.

To illustrate this with a simple example, let us see how $3+i$ factors in $\mathbb{Z}[i]$. We have $N(3+i) = (3+i)(3-i) = 10 = 2\cdot 5$. These two numbers factor as $2 = (i+i)(1-i)$ and $5 = (2+i)(2-i)$. These are prime factorizations in $\mathbb{Z}[i]$ since $N(1\pm i) = 2$ and $N(2\pm i) = 5$, both primes in $\mathbb{Z}$. Now we test whether for example $1+i$ divides $3+i$ by dividing:

$$\frac{3+i}{1+i} = \frac{(3+i)(1-i)}{(1+i)(1-i)} = \frac{4-2i}{2} = 2-i$$

Since the quotient $2-i$ is a Gaussian integer, we conclude that $1+i$ is a divisor of $3+i$ and we have the factorization $3+i = (1+i)(2-i)$. The is the prime factorization of $3+i$ since we have already noted that both $1+i$ and $2-i$ are primes in $\mathbb{Z}[i]$.

For a more complicated example consider $244+158i$. For a start, this factors as $2(122+79i)$. Since 122 and 79 have no common factors in $\mathbb{Z}$ we can't go any farther by factoring out ordinary integers. We know that 2 factors as $(1+i)(1-i)$ and these two factors are prime in $\mathbb{Z}[i]$ since their norm is 2. It remains to factor $122+79i$. This has norm $122^2+79^2 = 21125 = 5^3\cdot 13^2$. Both 5 and 13 happen to factor in $\mathbb{Z}[i]$, namely $5 = (2+i)(2-i)$ and $13 = (3+2i)(3-2i)$, and these are

prime factorizations since the norms of $2 \pm i$ and $3 \pm 2i$ are 5 and 13, primes in $\mathbb{Z}$. Thus we have the prime factorization

$$(122 + 79i)(122 - 79i) = 5^3 \cdot 13^2 = (2 + i)^3(2 - i)^3(3 + 2i)^2(3 - 2i)^2$$

Now we look at the factors on the right side of this equation to see which ones are factors of $122 + 79i$. Suppose for example we test whether $2 + i$ divides $122 + 79i$:

$$\frac{122 + 79i}{2 + i} = \frac{(122 + 79i)(2 - i)}{(2 + i)(2 - i)} = \frac{323 + 36i}{5}$$

This is not a Gaussian integer, so $2 + i$ does not divide $122 + 79i$. Let's try $2 - i$ instead:

$$\frac{122 + 79i}{2 - i} = \frac{(122 + 79i)(2 + i)}{(2 - i)(2 + i)} = \frac{165 + 280i}{5} = 33 + 56i$$

So $2-i$ does divide $122+79i$. In fact, we can expect that $(2-i)^3$ will divide $122+79i$, and it can be checked that it does. In a similar way one can check whether $3 + 2i$ or $3 - 2i$ divides $122 + 79i$, and one finds that it is $3 - 2i$ that divides $122 + 79i$, and in fact $(3 - 2i)^2$ divides $122 + 79i$. After these calculations one might expect that $122 + 79i$ was the product $(2 - i)^3(3 - 2i)^2$, but upon multiplying this product out one finds that it is the negative of $122 + 79i$, so

$$122 + 79i = (-1)(2 - i)^3(3 - 2i)^2$$

The factor -1 is a unit, so it could be combined with one of the other factors, for example changing one of the factors $2-i$ to $i-2$. Alternatively, we could replace the factor -1 by i^2 and then multiply each $3-2i$ factor by i to get the prime factorization

$$122 + 79i = (2 - i)^3(2 + 3i)^2$$

Hence for $244 + 158i$ we have the prime factorization

$$244 + 158i = (1 + i)(1 - i)(2 - i)^3(2 + 3i)^2$$

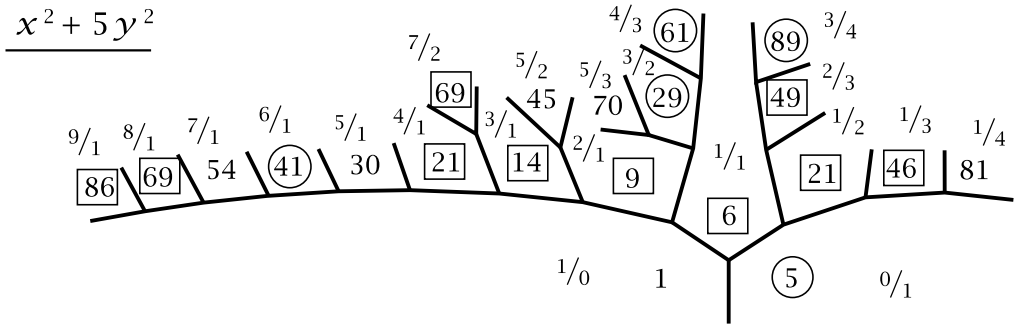
The question of uniqueness of prime decompositions in $\mathbb{Z}[\sqrt{D}]$ is much more subtle. Even if the ambiguity of inserting units is allowed, there are still cases when prime factorizations fail to be unique. One of the simplest instances is in $\mathbb{Z}[\sqrt{-5}]$ where we have the factorizations

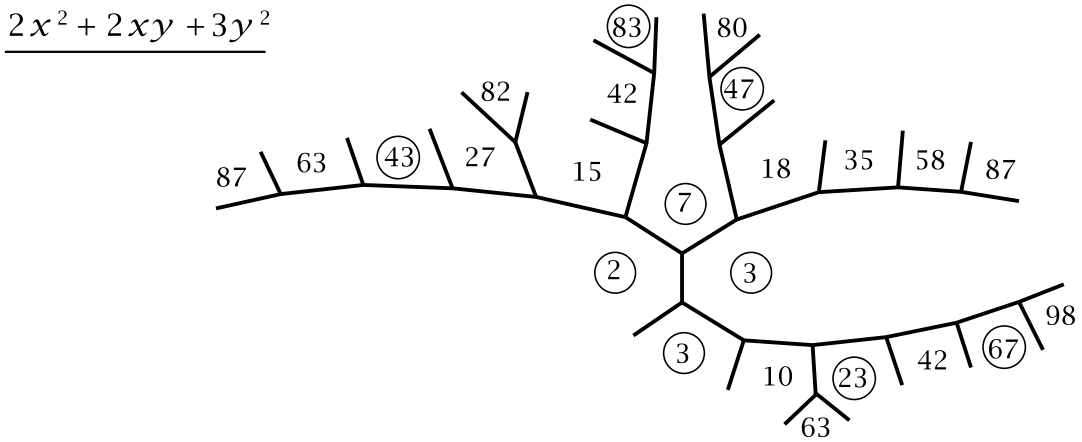
$$6 = (2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

The only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, so these two factorizations do not differ just by units. We can see that 2, 3, and $1 \pm \sqrt{-5}$ are prime in $\mathbb{Z}[\sqrt{-5}]$ by looking at norms. The norms of 2, 3, and $1 \pm \sqrt{-5}$ are 4, 9, and 6, so if one of 2, 3, or $1 \pm \sqrt{-5}$ was not a prime, it would have a factor of norm 2 or 3 since these are the only numbers that occur in nontrivial factorizations of 4, 9, and 6. However, the equations $x^2 + 5y^2 = 2$ and $x^2 + 5y^2 = 3$ have no integer solutions so there are no elements of $\mathbb{Z}[\sqrt{-5}]$ of

norm 2 or 3. Thus in $\mathbb{Z}[\sqrt{-5}]$ the number 6 has two prime factorizations that do not differ merely by units.

What is secretly going on in this example is that x^2+5y^2 is not the only quadratic form of discriminant -20, up to equivalence. Another form of the same discriminant is $2x^2+2xy+3y^2$, and this form takes on the values 2 and 3 that the form x^2+5y^2 omits, even though x^2+5y^2 does take on the value $6 = 2\cdot 3$. Here are the topographs of these two forms, with prime values circled and with boxes around nonprime values that yield nonunique prime factorizations:





In the topograph for x^2+5y^2 some numbers occur in boxes twice, leading to three different prime factorizations. For example 21 factors into primes in $\mathbb{Z}[\sqrt{-5}]$ as $3\cdot 7$, as $(1+2\sqrt{-5})(1-2\sqrt{-5})$ and as $(4+\sqrt{-5})(4-\sqrt{-5})$. Another example is $69 = 3\cdot 23 = (7+2\sqrt{-5})(7-2\sqrt{-5}) = (8+\sqrt{-5})(8-\sqrt{-5})$.

Proposition. *Let p be a prime in $\mathbb{Z}$. Then:*
(a) If either p or $-p$ is represented by the form x^2-Dy^2, so $p = \pm(a^2-Db^2)$, then $\pm p$ factors in $\mathbb{Z}[\sqrt{D}]$ as $p = \pm(a+b\sqrt{D})(a-b\sqrt{D})$ and both these factors are prime in ZD.
(b) If neither p nor $-p$ is represented by x^2-Dy^2 then p remains prime in $\mathbb{Z}[\sqrt{D}]$.

Proof: For part (a), if $p = \pm(a^2-Db^2)$, then certainly $\pm p$ factors in $\mathbb{Z}[\sqrt{D}]$ as $p = \pm(a+b\sqrt{D})(a-b\sqrt{D})$. The two factors are prime since their norm is $\pm p$ which is prime in $\mathbb{Z}$ by assumption.

For (b), if p is not a prime in $\mathbb{Z}[\sqrt{D}]$ then it factors in $\mathbb{Z}[\sqrt{D}]$ as $p = \alpha\beta$ with

neither α nor β a unit. Then $N(p) = p^2 = N(\alpha)N(\beta)$ with neither $N(\alpha)$ nor $N(\beta)$ equal to ± 1, hence we must have $N(\alpha) = \pm p$ and $N(\beta) = \pm p$. Focusing our attention just on α, this can be written as $a + b\sqrt{D}$, and then we have $\pm p = N(a + b\sqrt{D}) = a^2 - Db^2$, which says that the form $x^2 - Dy^2$ represents $\pm p$. Turning this statement around, it says that if $x^2 - Dy^2$ does not represent p or $-p$ then p is prime in $\mathbb{Z}[\sqrt{D}]$. □

Proposition. *If $\mathbb{Z}[\sqrt{D}]$ has unique factorization into primes then the only primes in $\mathbb{Z}[\sqrt{D}]$ are the primes described in (a) or (b) of the preceding proposition (or units times these primes).*

Proof: Let $\alpha = a + b\sqrt{D}$ be an arbitrary prime in $\mathbb{Z}[\sqrt{D}]$. The norm $n = N(\alpha) = (a+b\sqrt{D})(a-b\sqrt{D})$ is an integer in $\mathbb{Z}$ so it can be factored as a product $n = p_1 \cdots p_k$ of primes in $\mathbb{Z}$. Each p_i either stays prime in $\mathbb{Z}[\sqrt{D}]$ or factors as a product $(a_i + b_i\sqrt{D})(a_i - b_i\sqrt{D})$ of primes in $\mathbb{Z}[\sqrt{D}]$. This gives a factorization of n into primes in $\mathbb{Z}[\sqrt{D}]$. A second factorization of n into primes in $\mathbb{Z}[\sqrt{D}]$ can be obtained from the formula $n = (a + b\sqrt{D})(a - b\sqrt{D})$ by factoring the second factor into primes, since the first factor $a + b\sqrt{D}$ is already prime by assumption. (In fact if $a + b\sqrt{D}$ is prime then $a - b\sqrt{D}$ will also be a prime, but we don't need to know this.) If we have unique factorization in $\mathbb{Z}[\sqrt{D}]$ then the prime factor $a + b\sqrt{D}$ of n will have to be one of the prime factors in the first prime factorization of n, or a unit times one of these primes. Thus $a + b\sqrt{D}$ will be a unit times a prime of one of the two types described in the previous proposition. □

Unique Factorization via the Euclidean Algorithm

Our goal now is to show that unique factorization holds for the Gaussian integers $\mathbb{Z}[i]$, and in a few other cases as well. The plan will be to see that Gaussian integers have a Euclidean algorithm much like the Euclidean algorithm in $\mathbb{Z}$, then deduce unique factorization from this Euclidean algorithem.

In order to prove that prime factorizations are unique we will use the following special property that holds in $\mathbb{Z}$ and in some other rings $\mathbb{Z}[\sqrt{D}]$ as well:

$(*)$ *If a prime p divides a product ab then p must divide either a or b.*

One way to prove this for $\mathbb{Z}$ would be to consider the prime factorization of ab, which can be obtained by factoring each of a and b into primes separately. Then if the prime p divides ab, it would have to occur in the prime factorization of ab, hence it would occur in the prime factorization of either a or b, which would say that p divides a or b.

This argument assumed implicitly that the prime factorization of ab was unique. Thus the property $(*)$ is a consequence of unique factorization into primes. But the

property $(*)$ also implies that prime factorizations are unique. To see why, consider two prime factorizations of a number n:

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$$

We can assume $k \le l$ by interchanging the p_i's and q_i's if necessary. We want to argue that if $(*)$ holds for each p_i, then the q_i's are just a permutation of the p_i's and in particular $k = l$. The argument to prove this goes as follows. Consider first the prime p_1. This divides the product $q_1(q_2 \cdots q_l)$ so by property $(*)$ it divides either q_1 or $q_2 q_3 \cdots q_l$. In the latter case, another application of $(*)$ shows that p_1 divides either q_2 or $q_3 q_4 \cdots q_l$. Repeating this argument as often as necessary, we conclude that p_1 must divide at least one q_i. After permuting the q_i's we can assume that p_1 divides q_1. If we are assuming all the p_i's and q_i's are positive integers, the fact that the prime p_1 divides the prime q_1 implies that p_1 equals q_1, so we can cancel p_1 and q_1 from the equation $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ to get $p_2 \cdots p_k = q_2 \cdots q_l$. Now repeat the argument to show that p_2 equals some remaining q_i which we can assume is q_2 after a permutation. After further repetitions we eventually reach the point that the final p_k is a product of the remaining q_i's. But then since p_k is prime there could only be one remaining q_i, so we would have $k = l$ and $p_k = q_k$, finishing the argument.

If we knew the analog of property $(*)$ held for primes in $\mathbb{Z}[\sqrt{D}]$ we could make essentially the same argument to show that unique factorization holds in $\mathbb{Z}[\sqrt{D}]$. The only difference in the argument would be that we would have to take units into account. The argument would be exactly the same up to the point where we concluded that p_1 divides q_1. Then the fact that q_1 is prime would not say that p_1 and q_1 were equal, but only that q_1 is a unit times p_1, so we would have an equation $q_1 = e p_1$ with e a unit. Then we would have $p_1 p_2 \cdots p_k = e p_1 q_2 \cdots q_l$. Canceling p_1 would then yield $p_2 p_3 \cdots p_k = e q_2 q_3 \cdots q_l$. The product $e q_2$ is prime if q_2 is prime, so if we let $q_2' = e q_2$ we would have $p_2 p_3 \cdots p_k = q_2' q_3 \cdots q_l$. The argument could then be repeated to show eventually that the q_i's are the same as the p_i's up to permutation and multiplication by units, which is what unique factorization means.

Since the property $(*)$ implies unique factorization, it will not hold in $\mathbb{Z}[\sqrt{D}]$ when $\mathbb{Z}[\sqrt{D}]$ does not have unique factorization. For a concrete example consider $\mathbb{Z}[\sqrt{-5}]$. Here we had nonunique prime factorizations $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. The prime 2 thus divides the product $(1+\sqrt{-5})(1-\sqrt{-5})$ but it does not divide either factor $1 \pm \sqrt{-5}$ since $(1 \pm \sqrt{-5})/2$ is not an element of $\mathbb{Z}[\sqrt{-5}]$.

For $\mathbb{Z}$ we know from Chapter 2 that an equation $ax + by = 1$ always has solutions in $\mathbb{Z}$ whenever a and b have no common factors. This fact can be used to deduce that property $(*)$ holds in $\mathbb{Z}$. To see this, suppose that a prime p divides a product ab. It will suffice to show that if p does not divide a then it must divide b. If p does not divide a, then since p is prime, p and a have no common factors. This implies

that the equation $px + ay = 1$ is solvable with integers x and y. Now multiply this equation by b to get an equation $b = pbx + aby$. The number p divides the right side of this equation since it obviously divides pbx and it divides ab by assumption. Hence p divides b, which is what we wanted to show. Thus we have (finally!) proved that $\mathbb{Z}$ has unique factorization.

How did we know that equations $ax + by = 1$ in $\mathbb{Z}$ are solvable when a and b have no common factors? We deduced this from properties of continued fractions and the Farey diagram, but these ultimately came from the Euclidean algorithm. In fact it is not hard to deduce solvability of $ax + by = 1$ directly from the Euclidean algorithm.

What the Euclidean algorithm gives us, in the case of $\mathbb{Z}$, is a method for starting with two positive integers α_0 and α_1 and constructing a sequence of positive numbers α_i and β_i satisfying equations

$$\begin{aligned}
\alpha_0 &= \beta_1\alpha_1 + \alpha_2 \\
\alpha_1 &= \beta_2\alpha_2 + \alpha_3 \\
&\vdots \\
\alpha_{n-2} &= \beta_{n-1}\alpha_{n-1} + \alpha_n \\
\alpha_{n-1} &= \beta_n\alpha_n + \alpha_{n+1} \\
\alpha_n &= \beta_{n+1}\alpha_{n+1}
\end{aligned}$$

From these equations we can deduce two consequences:

(1) α_{n+1} divides α_0 and α_1.
(2) The equation $\alpha_{n+1} = \alpha_0 x + \alpha_1 y$ is solvable in $\mathbb{Z}$.

To see why (1) is true, note that the last equation implies that α_{n+1} divides α_n. Then the next-to-last equation implies that α_{n+1} divides α_{n-1}, and the equation before this then implies that α_{n+1} divides α_{n-2}, and so on until one deduces that α_{n+1} divides all the α_i's and in particular α_0 and α_1.

To see why (2) is true, observe that each equation before the last one allows an α_i to be expressed as a linear combination of α_{i-1} and α_{i-2}, so by repeatedly substituting in, one can express each α_i in terms of α_0 and α_1 as a linear combination $x\alpha_0 + y\alpha_1$ with integer coefficients x and y, so in particular α_{n+1} can be represented in this way, which says that the equation $\alpha_{n+1} = \alpha_0 x + \alpha_1 y$ is solvable in $\mathbb{Z}$.

Now if we assume that α_0 and α_1 have no common divisors except 1, then α_{n+1} must by 1 by statement (1), and by statement (2) we get integers x and y such that $\alpha_0 x + \alpha_1 y = 1$, as we wanted. In this way we see that the Euclidean algorithm in $\mathbb{Z}$ implies unique factorization.

A very similar argument works in $\mathbb{Z}[\sqrt{D}]$ provided that one has a Euclidean algorithm to produce the sequence of equations above starting with any nonzero pair of elements α_0 and α_1 in $\mathbb{Z}[\sqrt{D}]$. The only difference in the more general case is that

α_{n+1} might not be 1, but only a unit in $\mathbb{Z}[\sqrt{D}]$. Thus one would apply statements (1) and (2) to a pair α_0, α_1 whose only common divisors were units, hence α_{n+1} would be a unit, and then the equation $\alpha_{n+1} = \alpha_0 x + \alpha_1 y$ could be modified by multiplying through by α_{n+1}^{-1} to get an equation $1 = \alpha_0 x + \alpha_1 y$ with solutions x, y in $\mathbb{Z}[\sqrt{D}]$. As we have seen earlier, this would imply unique factorization in $\mathbb{Z}[\sqrt{D}]$.

Let us show now that there is a Euclidean algorithm in the Gaussian integers $\mathbb{Z}[i]$. The key step is to be able to find, for each pair of nonzero Gaussian integers α_0 and α_1, two more Gaussian integers β_1 and α_2 such that $\alpha_0 = \beta_1\alpha_1 + \alpha_2$ and $N(\alpha_2) < N(\alpha_1)$. If we can always do this, then by repeating the same step over and over we construct a sequence of α_i's and β_i's where the successive α_i's have smaller and smaller norms. Since these norms are positive integers, they cannot keep decreasing infinitely often, so eventually the process will reach an α_i of norm 0, so this α_i must be 0 and the Euclidean algorithm will end in a finite number of steps, as it should.

The equation $\alpha_0 = \beta_1\alpha_1 + \alpha_2$ is saying that when we divide α_1 into α_0, we obtain a quotient β_1 and a remainder α_2. What we want is for the remainder to be 'smaller' than the divisor α_1, in the sense of having a smaller norm. To get an idea how we can do this it may be helpful to look at the equivalent equation

$$\frac{\alpha_0}{\alpha_1} = \beta_1 + \frac{\alpha_2}{\alpha_1}$$

If we were working with ordinary integers, the quotient β_1 would be the integer part of the rational number α_0/α_1 and α_2/α_1 would be the remaining fractional part. For Gaussian integers we do something similar, but instead of taking β_1 to be the 'integer part' of α_0/α_1 we take it to be the *closest* Gaussian integer to α_0/α_1.

Here is an example, where we choose α_0 to be $12 + 15i$ and α_1 to be $5 + 2i$. Then:

$$\frac{\alpha_0}{\alpha_1} = \frac{12+15i}{5+2i} = \frac{(12+15i)(5-2i)}{(5+2i)(5-2i)} = \frac{90+51i}{29} = (3+2i) + \frac{3-7i}{29}$$

Here in the last step we chose $3 + 2i$ as β_1 because 3 is the closest integer to $90/29$ and 2 is the closest integer to $51/29$. Having found a likely candidate for β_1, we can use the equation $\alpha_0 = \beta_1\alpha_1 + \alpha_2$ to find α_2. This equation is

$$12 + 15i = (3+2i)(5+2i) + \alpha_2 = (11+16i) + \alpha_2 \qquad \text{hence} \qquad \alpha_2 = 1 - i$$

Notice that $N(1-i) = 2 < N(5+2i) = 29$ so we have $N(\alpha_2) < N(\alpha_1)$ as we wanted.

Will the process of choosing β_1 as the nearest Gaussian integer to the 'Gaussian rational' α_0/α_1 always lead to an α_2 with $N(\alpha_2) < N(\alpha_1)$? The answer is yes because if we write the quotient α_2/α_1 in the form $x + yi$ for rational numbers x and y (in the example above we have $x + yi = \frac{3}{29} + \frac{-7}{29}i$) then having β_1 the closest Gaussian integer to α_0/α_1 says that $|x| \le \frac{1}{2}$ and $|y| \le \frac{1}{2}$, so

$$N\Big(\frac{\alpha_2}{\alpha_1}\Big) = x^2 + y^2 \le \frac{1}{4} + \frac{1}{4} < 1$$

and hence

$$N(\alpha_2) = N\Big(\frac{\alpha_2}{\alpha_1} \cdot \alpha_1\Big) = N\Big(\frac{\alpha_2}{\alpha_1}\Big)N(\alpha_1) < N(\alpha_1)$$

This shows that there is a general Euclidean algorithm in $\mathbb{Z}[i]$, hence $\mathbb{Z}[i]$ has unique factorization.

Let us finish carrying out the Euclidean algorithm for $\alpha_0 = 12 + 15i$ and $\alpha_1 = 5 + 2i$. The next step is to divide $\alpha_2 = 1 - i$ into $\alpha_1 = 5 + 2i$:

$$\frac{5+2i}{1-i} = \frac{(5+2i)(1+i)}{(1-i)(1+i)} = \frac{3+7i}{2} = (1+3i) + \frac{1+i}{2}$$

Notice that the fractions $3/2$ and $7/2$ are exactly halfway between two consecutive integers, so instead of choosing $1 + 3i$ for the closest integer to $(3 + 7i)/2$ we could equally well have chosen $2 + 3i$, $1 + 4i$, or $2 + 4i$. If we stick with the choice $1 + 3i$ then we use this to calculate the next α_i:

$$5 + 2i = (1 + 3i)(1 - i) + \alpha_3 = (4 + 2i) + \alpha_3 \qquad \text{hence} \qquad \alpha_3 = 1$$

The final step would be simply to write $1 - i = (1 - i)1 + 0$. Thus the full Euclidean algorithm is:

$$\begin{aligned} 12 + 15i &= (3 + 2i)(5 + 2i) + (1 - i) \\ 5 + 2i &= (1 + 3i)(1 - i) + 1 \\ 1 - i &= (1 - i)1 + 0 \end{aligned}$$

In particular, since the last nonzero remainder is 1, a unit in $\mathbb{Z}[i]$, we deduce that this is the greatest common divisor of $12 + 15i$ and $5 + 2i$, where 'greatest' means 'of greatest norm'. In other words $12 + 15i$ and $5 + 2i$ have no common divisors other than units.

As in the case of ordinary integers, the equations that display the results of carrying out the Euclidean algorithm can be used to express the last nonzero remainder in terms of the original two numbers:

$$\begin{aligned} 1 &= (5 + 2i) - (1 + 3i)(1 - i) \\ &= (5 + 2i) - (1 + 3i)[(12 + 15i) - (3 + 2i)(5 + 2i)] \\ &= -(1 + 3i)(12 + 15i) + (-2 + 11i)(5 + 2i) \end{aligned}$$

If it had happened that the last nonzero remainder was a unit other than 1, we could have expressed this unit in terms of the original two Gaussian integers, and then multiplied the equation by the inverse of the unit to get an expression for 1 in terms of the original two Gaussian integers.

Other Instances of Unique Factorization

Elements of $\mathbb{Z}[\sqrt{-2}]$ factor uniquely into primes because there is a Euclidean algorithm in $\mathbb{Z}[\sqrt{-2}]$. The crucial point we used in the verification that $\mathbb{Z}[i]$ had a Euclidean algorithm was that each complex number is within a distance less than 1 from some Gaussian integer. The same thing is true for $\mathbb{Z}[\sqrt{-2}]$ since the numbers in $\mathbb{Z}[\sqrt{-2}]$ form a rectangular lattice in the plane, where the rectangles have width 1 and height $\sqrt{2}$. Every point in such a rectangle is at distance less than 1 from one of the four vertices since the worst case is the center point of the rectangle, which is at distance $\sqrt{3}/2$ from the vertices.

This argument does not work in $\mathbb{Z}[\sqrt{-3}]$ since in a rectangle of width 1 and height $\sqrt{3}$ the center point is at distance exactly 1 from the vertices, and one needs distance strictly less than 1 for the Euclidean algorithm. In fact unique factorization fails in $\mathbb{Z}[\sqrt{-3}]$, and in many other cases too:

Proposition. *Unique factorization fails in $\mathbb{Z}[\sqrt{D}]$ whenever $D < -2$, and it also fails when $D > 0$ and $D \equiv 1$ modulo 4. (In the latter case we assume as always that D is not a square).*

Proof: The number $D^2 - D$ factors in $\mathbb{Z}[\sqrt{D}]$ as $(D + \sqrt{D})(D - \sqrt{D})$, and it also factors as $D(D-1)$. The number 2 divides either D or $D-1$ since one of these two consecutive integers must be even. However, 2 does not divide either $D + \sqrt{D}$ or $D - \sqrt{D}$ in $\mathbb{Z}[\sqrt{D}]$ since $(D \pm \sqrt{D})/2$ is not an element of $\mathbb{Z}[\sqrt{D}]$ as the coefficient of $\sqrt{D}$ in this quotient is not an integer. If we knew that 2 was prime in $\mathbb{Z}[\sqrt{D}]$ we would then have two distinct factorizations of $D^2 - D$ into primes in $\mathbb{Z}[\sqrt{D}]$: One obtained by combining prime factorizations of D and $D-1$, and the other obtained by combining prime factorizations of $D + \sqrt{D}$ and $D - \sqrt{D}$. The first factorization would contain the prime 2 and the second would not.

It remains to check that 2 is a prime in $\mathbb{Z}[\sqrt{D}]$ in the cases listed. If it is not a prime, then it factors as $2 = \alpha\beta$ with neither α nor β a unit, so we would have $N(\alpha) = N(\beta) = \pm 2$. Thus the equation $x^2 - Dy^2 = \pm 2$ would have an integer solution (x, y). This is clearly impossible if $D = -3$ or any negative integer less than -3. If $D > 0$ and $D \equiv 1$ modulo 4 then if we look at the equation $x^2 - Dy^2 = \pm 2$ modulo 4 it becomes $x^2 - y^2 \equiv 2$, but this is impossible since x^2 and y^2 are congruent to 0 or 1 modulo 4, so $x^2 - y^2$ is congruent to 0, 1, or -1. □

In the cases $D \equiv 1$ modulo 4 there is a way to enlarge $\mathbb{Z}[\sqrt{D}]$ to a slightly larger ring $\mathbb{Z}[\omega]$ which sometimes has unique factorization when $\mathbb{Z}[\sqrt{D}]$ does not. The construction also fills a gap by providing a norm form whose discriminant is congruent to 1 modulo 4, complementing the norm form $x^2 - Dy^2$ of discriminant $4D \equiv 0$ modulo 4. The new norm form will be $x^2 + xy - dy^2$, of discriminant $1 + 4d$.

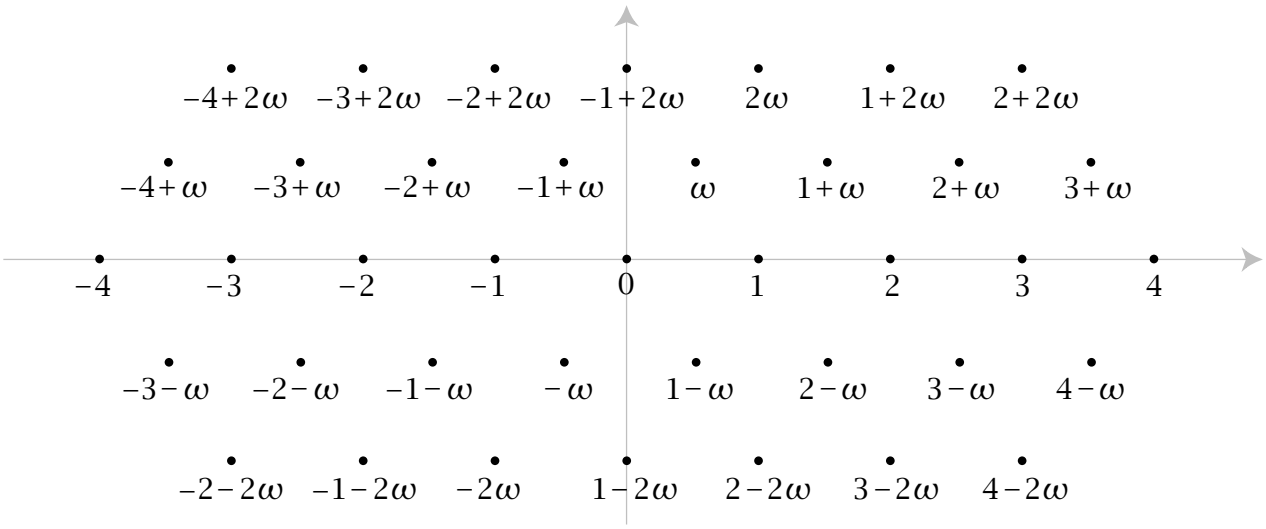
The number $\omega = (1 + \sqrt{1 + 4d})/2$ satisfies the quadratic equation $\omega^2 - \omega - d = 0$, whose other root is $\overline{\omega} = (1 - \sqrt{1 + 4d})/2$. From the quadratic equation we obtain the

relation $\omega^2 = \omega + d$, and this implies that the set $\mathbb{Z}[\omega] = \{x + y\omega \mid x, y \in \mathbb{Z}\}$ is closed under multiplication and hence forms a ring, like $\mathbb{Z}[\sqrt{D}]$. The norm in $\mathbb{Z}[\omega]$ is defined by

$$\begin{aligned} N(x + y\omega) = (x + y\omega)(x + y\overline{\omega}) &= x^2 + xy(\omega + \overline{\omega}) + y^2\omega\overline{\omega} \\ &= x^2 + xy - dy^2 \end{aligned}$$

since $\omega + \overline{\omega} = 1$ and $\omega\overline{\omega} = -d$. This norm function still satisfies the key property $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in \mathbb{Z}[\omega]$ since it is in fact just the restriction of the earlier norm to the subring $\mathbb{Z}[\omega]$ of $\mathbb{Q}(\sqrt{1 + 4d})$.

For example, when $d = -1$ we have $\omega = (1 + \sqrt{-3})/2$ and the elements of $\mathbb{Z}[\omega]$ form a lattice of equilateral triangles in the xy-plane:



When $\omega = (1 + \sqrt{-3})/2$ there is a Euclidean algorithm in $\mathbb{Z}[\omega]$ since every complex number is within distance less than 1 of some element of $\mathbb{Z}[\omega]$. Hence unique factorization holds in $\mathbb{Z}[\omega]$. There are six units, the six lattice points of distance 1 from the origin, which are the numbers ± 1, $\pm\omega$, and $\pm(\omega - 1)$. Equivalently, these are the powers ω^n for $n = 0, 1, 2, 3, 4, 5$, with $\omega^6 = 1$. The norm in $\mathbb{Z}[\omega]$ is given by the formula $N(x + y\omega) = x^2 + xy + y^2$. The primes p in $\mathbb{Z}$ that factor in $\mathbb{Z}[\omega]$ are those that can be written in the form $p = x^2 + xy + y^2 = N(x + y\omega)$. The analog of Fermat's theorem in this context is the fact that the primes p that can be written as $x^2 + xy + y^2$ are $p = 3$ and the primes $p = 3k + 1$. For example $3 = N(1 + \omega)$, $7 = N(2 + \omega)$, $13 = N(3 + \omega)$, and $17 = N(3 + 2\omega)$. The factorization in each of these cases is given by the formula $p = N(x + y\omega) = (x + y\omega)(x + y\overline{\omega})$.

For larger negative values of d the picture of $\mathbb{Z}[\omega]$ in the complex plane is similar but stretched in the vertical direction. It is not hard to do the measurements to show that $\mathbb{Z}[\omega]$ is Euclidean only in the three cases $d = -1, -2, -3$ when the discriminant $\Delta = 1 + 4d$ is $-3, -7, -11$. There are four other negative values of the discriminant when $\mathbb{Z}[\omega]$ has unique factorization even though it does not have a Euclidean algorithm, the discriminants $\Delta = -19, -43, -67, -163$. Together with $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ this brings the total number of negative discriminants for which $\mathbb{Z}[\sqrt{D}]$ or $\mathbb{Z}[\omega]$ has

unique factorization to nine, the discriminants

$$\Delta = -3, -4, -7, -8, -11, -19, -43, -67, -163$$

These are exactly the nine negative discriminants for which all quadratic forms of that discriminant are equivalent. (This is not an accident.)

At first glance the choice of ω as $(1 + \sqrt{1 + 4d})/2$ might seem somewhat arbitrary, and one might wonder whether similar constructions using other denominators besides 2 would also be possible. In order to do multiplication within the set $\mathbb{Z}[\omega]$ of complex numbers $x + y\omega$ with x and y integers one must be able to express ω^2 in this form as $m\omega + n$, so ω must satisfy a quadratic equation $\omega^2 - m\omega - n = 0$. This has roots $(m \pm \sqrt{m^2 + 4n})/2$, so we see that larger denominators than 2 will not work. If m is even, say $m = 2k$, then ω becomes $k \pm \sqrt{k^2 + n}$, with no denominators at all. If m is odd, $m = 2k + 1$, then ω is $(2k + 1 \pm \sqrt{4k^2 + 4k + 1 + 4n})/2$, which can be written as $k + (1 + \sqrt{1 + 4d})/2$ so we are actually in the situation already considered.

We have seen that enlarging the ring $\mathbb{Z}[\sqrt{D}]$ to $\mathbb{Z}[\omega]$ in the cases $D = 1 + 4d$ can sometimes restore unique factorization. Another sort of enlargement comes from the fact that $\mathbb{Z}[\sqrt{n^2 D}]$ is contained in $\mathbb{Z}[\sqrt{D}]$. For example $\mathbb{Z}[\sqrt{-8}]$, which does not have unique factorization, is contained in $\mathbb{Z}[\sqrt{-2}]$ which does. For this reason it is often best to restrict attention to integers D having no square factors, and in this case we unify the notation by letting R_D denote the ring $\mathbb{Z}[\sqrt{D}]$ if $D \neq 1 + 4d$ and $\mathbb{Z}[\omega]$ if $D = 1 + 4d$. The discriminant of R_D is then D when $D = 1 + 4d$ and $4D$ when $D \neq 1 + 4d$.

When the discriminant is positive, R_D is a subring of the real numbers, so it is somewhat paradoxical that these cases tend to be more complex than in the case of negative discriminant, when R_D contains complex numbers. One reason for the added complication is that the norm form $x^2 - Dy^2$ or $x^2 + xy - dy^2$ is a hyperbolic form rather than elliptic. In particular, this means that norms can be negative as well as positive, and the norm doesn't have the nice geometric meaning of the square of the distance to the origin that it has in the imaginary case. Since the norm can be negative, the definition of a Euclidean algorithm is modified so that in the equations $\alpha_{i-1} = \beta_i \alpha_i + \alpha_{i+1}$ it is required that $|N(\alpha_{i+1})| < |N(\alpha_i)|$. It is known that there are exactly 16 positive values of D for which there is a Euclidean algorithm in R_D:

$$2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

In these cases one has unique factorization, but there are 22 other values of $D < 100$ where unique factorization holds even though there is no Euclidean algorithm:

$$14, 22, 23, 31, 38, 43, 46, 47, 53, 59, 61, 62, 67, 69, 71, 77, 83, 86, 89, 93, 94, 97$$

It is still not known whether there are infinitely many values of D where there is unique factorization, although it is known that there are infinitely many values of D for which unique factorization fails.

Exercises

1. (a) Show that if α and β are elements of $\mathbb{Z}[\sqrt{D}]$ such that α is a unit times β, then $N(\alpha) = \pm N(\beta)$.
(b) Either prove or give a counterexample to the following statement: If α and β are Gaussian integers with $N(\alpha) = N(\beta)$ then α is a unit times β.

2. Show that a Gaussian integer $x + yi$ with both x and y odd is divisible by $1 + i$ but not by $(1 + i)^2$.

3. There are four different ways to write the number $1105 = 5 \cdot 13 \cdot 17$ as a sum of two squares. Find these four ways using the factorization of 1105 into primes in $\mathbb{Z}[i]$. [Here we are not counting $5^2 + 2^2$ and $2^2 + 5^2$ as different ways of expressing 29 as the sum of two squares. Note that an equation $n = a^2 + b^2$ is equivalent to an equation $n = (a + bi)(a - bi)$.]

4. (a) Find four different units in $\mathbb{Z}[\sqrt{3}]$ that are positive real numbers, and find four that are negative.
(b) Do the same for $\mathbb{Z}[\sqrt{11}]$.

5. Make a list of all the Gaussian primes $x + yi$ with $-7 \le x \le 7$ and $-7 \le y \le 7$. (The only actual work here is to figure out the primes $x + yi$ with $0 \le y \le x \le 7$, then the rest are obtainable from these by symmetry properties.)

6. Factor the following Gaussian integers into primes in $\mathbb{Z}[i]$: $3 + 5i$, $8 - i$, $10 + i$, $5 - 12i$, $35i$, $-35 + 120i$, $253 + 204i$.

7. In this problem we consider $\mathbb{Z}[\sqrt{-2}]$. To simplify notation, let $\omega = \sqrt{-2}$, so elements of $\mathbb{Z}[\omega]$ are sums $x + y\omega$ with $x, y \in \mathbb{Z}$ and with $\omega^2 = -2$. We have $N(x + y\omega) = x^2 + 2y^2 = (x + y\omega)(x - y\omega)$.

(a) Draw the topograph of $x^2 + 2y^2$ including all values less than 70 (by symmetry, it suffices to draw just the upper half of the topograph). Circle the values that are prime (prime in $\mathbb{Z}$, that is). Also label each region with its x/y fraction.

(b) Which primes in $\mathbb{Z}$ factor in $\mathbb{Z}[\omega]$?

(c) Using the information in part (a), list all primes in $\mathbb{Z}[\omega]$ of norm less than 70.

(d) Draw a diagram in the xy-plane showing all elements $x + y\omega$ in $\mathbb{Z}[\omega]$ of norm less than 70 as small dots, with larger dots or squares for the elements that are prime in $\mathbb{Z}[\omega]$. (There is symmetry, so the primes in the first quadrant determine the primes in the other quadrants.)

(e) Show that the only primes $x + y\omega$ in $\mathbb{Z}[\omega]$ with x even are $\pm\omega$. (Your diagram in part (d) should give some evidence that this is true.)

(f) Factor $4 + \omega$ into primes in $\mathbb{Z}[\omega]$.